Cisco ASR 5x00 Release Change Reference
Version 15.0

Last Updated February 27, 2015
The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB’s public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

Notwithstanding any other warranty herein, all document files and software of these suppliers are provided “as is” with all faults. Cisco and the above-named suppliers disclaim all warranties, expressed or implied, including, without limitation, those of merchantability, fitness for a particular purpose and noninfringement or arising from a course of dealing, usage, or trade practice.

In no event shall Cisco or its suppliers be liable for any indirect, special, consequential, or incidental damages, including, without limitation, lost profits or loss or damage to data arising out of the use or inability to use this manual, even if Cisco or its suppliers have been advised of the possibility of such damages.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.

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

Cisco ASR 5x00 Release Change Reference

© 2015 Cisco Systems, Inc. All rights reserved.
CONTENTS

About this Guide ........................................................................................................... XXV
  Conventions Used ........................................................................................................ xxvi
  Supported Documents and Resources ...................................................................... xxvii
  Related Documentation ............................................................................................ xxvii
  Obtaining Documentation ......................................................................................... xxvii
  Contacting Customer Support ................................................................................ xxviii

AAA Changes in Release 15.0 ....................................................................................... 29

AAA Enhancements for February 27, 2015 ................................................................. 30
  CSCur43509 - PCEF is not triggering 29 as APN-AMBR mod failure in CCR .......... 30
  Feature Changes ...................................................................................................... 30

AAA Enhancements for March 31, 2014 ................................................................. 31
  CSCur89572, CSCus36547, CSCur13994 - Diameter support for 'EPS-Location-Information' AVP 30
  Feature Changes ...................................................................................................... 30

AAA Enhancements for April 30, 2014 ................................................................. 31
  CSCup75566 - Add CC-Group AVP in Gx Dictionary for Customer ....................... 31
  Feature Changes ...................................................................................................... 31

AAA Enhancements for June 6, 2014 ................................................................. 32
  CSCuq06614 - Radius AVP SN-Rad-APN-Name to be added in custom67 ................. 31
  Feature Changes ...................................................................................................... 32

AAA Enhancements for October 31, 2014 ............................................................... 33
  CSCui07715 - ASR5000 sends CCR-T before CCA-U arrived for CCR-U .............. 31
  Feature Changes ...................................................................................................... 33

AAA Enhancements for November 30, 2013 ........................................................... 39
  CSCuh51285 - Always send Supported-Features AVP in CCR-U ......................... 39
  Feature Changes ...................................................................................................... 39

AAA Enhancements for December 31, 2014 .......................................................... 39
  CSCuh96548 - Send 3GPP-Charging-Characteristics in CCR-I over Gx ............... 39
  Feature Changes ...................................................................................................... 39

AAA Enhancements for January 31, 2015 .............................................................. 40
  CSCul89329 - dpcacustom24:call dropped if Supported-feature AVP absent in CCR-I . 40
  Feature Changes ...................................................................................................... 40

AAA Enhancements for February 27, 2015 ............................................................... 41
ADC Enhancements for February 28, 2014 ................................................ 41
Feature Changes ................................................................................. 41
CSCud80426, CSCud28221 - PCC-Level report is not triggered when same mon-key for sess/pcc is used 41
Feature Changes ................................................................................. 41
CSCue65856 - Local-policy to support TFT based on UE address request type ...................... 42
Feature Changes ................................................................................. 42
Command Changes ............................................................................... 42
Performance Changes ......................................................................... 42
CSCuh84653 - Gx: RAT-Type: EHRPD (2003) support required for eHRPD call ................... 42
Feature Changes ................................................................................. 43
CSCui30541 - Subscription-ID AVP in CCR-I does not support MSISDN for RAT-type WLAN 43
Feature Changes ................................................................................. 43
Command Changes ............................................................................... 43
CSCuj16170 - IPSG does not update Timezone over Gx for RAT Type WLAN .................... 44
Feature Changes ................................................................................. 44
CSCuj20238 - [Gn-Gp] - 3GPP-User-Location-Info missing in 2nd INTERIM SDC-3g-4g-3g HO 44
Feature Changes ................................................................................. 44
CSCui54761 - PGW: Gx rel 10 packet filter - Wrong TFT in CREATE_BEARER_REQUEST 44
Feature Changes ................................................................................. 44
CSCui97199 - CCR-T is not triggered when 5003 error is received ................................. 45
Feature Changes ................................................................................. 45
Feature Changes ............................................................................... 45
AAA Enhancements for September 30, 2013 ................................................ 46
Diameter Accounting Management Changes as of September 30, 2013 ........................ 46
Diameter Feature Changes ..................................................................... 46
Diameter Command Changes ................................................................ 58
Diameter Attribute Changes ................................................................ 75
Diameter Performance Indicator Changes ........................................... 76
RADIUS Accounting Management Changes as of September 30, 2013 ......................... 85
RADIUS Feature Changes .................................................................... 85
RADIUS Command Changes ................................................................. 86
RADIUS Attribute Changes .................................................................. 87
RADIUS Performance Management Changes ....................................... 89

ADC Changes in Release 15.0 .................................................................. 91
ADC Enhancements for February 28, 2014 ................................................ 92
CSCui125213 - Add Support for BBM app in iOS and Android ................................. 92
Feature Changes ................................................................................. 92
Command Changes ............................................................................... 92
Performance Indicator Changes ........................................................... 93
CSCui99411 - Support BOX application in ADC ....................................... 95
Feature Changes ................................................................................. 95
Command Changes ............................................................................... 95
Performance Indicator Changes ........................................................... 96
CSCui82621 - Support for Chikka mail and IM in p2p plugin ............................... 97
Feature Changes ................................................................................. 97
Command Changes ............................................................................... 97
Performance Indicator Changes ........................................................... 98
CSCui82673 - Support for imgur in p2p plugin ......................................... 99
Feature Changes ................................................................................. 99
Command Changes ............................................................................... 100
Performance Indicator Changes ........................................................... 101
CSCui82626 - Support for Oist in p2p plugin ........................................ 102
Feature Changes ............................................................................... 102
Command Changes ............................................................................... 102
<table>
<thead>
<tr>
<th>ADC Enhancements for September 30, 2013</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCuI82671 - Support for regram in p2p plugin</td>
<td>103</td>
</tr>
<tr>
<td>Feature Changes</td>
<td>104</td>
</tr>
<tr>
<td>Command Changes</td>
<td>104</td>
</tr>
<tr>
<td>Performance Indicator Changes</td>
<td>105</td>
</tr>
<tr>
<td>CSCuI72953 - Support for additional P2P protocol in ADC</td>
<td>106</td>
</tr>
<tr>
<td>Feature Changes</td>
<td>106</td>
</tr>
<tr>
<td>Command Changes</td>
<td>107</td>
</tr>
<tr>
<td>Performance Indicator Changes</td>
<td>108</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ADC Enhancements for December 20, 2013</th>
<th>110</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCuIg26539 - Support for JAP in the p2p plugin</td>
<td>110</td>
</tr>
<tr>
<td>Feature Changes</td>
<td>110</td>
</tr>
<tr>
<td>Command Changes</td>
<td>110</td>
</tr>
<tr>
<td>Performance Indicator Changes</td>
<td>111</td>
</tr>
<tr>
<td>CSCuIh57347 - ADC Support Monkey3</td>
<td>112</td>
</tr>
<tr>
<td>Feature Changes</td>
<td>112</td>
</tr>
<tr>
<td>Command Changes</td>
<td>113</td>
</tr>
<tr>
<td>Performance Indicator Changes</td>
<td>114</td>
</tr>
<tr>
<td>CSCuI57348 - Add Support for Facebook Voice in iOS and Android Apps</td>
<td>115</td>
</tr>
<tr>
<td>Feature Changes</td>
<td>115</td>
</tr>
<tr>
<td>Command Changes</td>
<td>115</td>
</tr>
<tr>
<td>Performance Indicator Changes</td>
<td>115</td>
</tr>
<tr>
<td>CSCuI93029 - Apple Maps support in P2P Protocol</td>
<td>116</td>
</tr>
<tr>
<td>Feature Changes</td>
<td>116</td>
</tr>
<tr>
<td>Command Changes</td>
<td>116</td>
</tr>
<tr>
<td>Performance Indicator Changes</td>
<td>117</td>
</tr>
<tr>
<td>CSCuIj44380 - Support yahoo mail in P2P detection</td>
<td>118</td>
</tr>
<tr>
<td>Feature Changes</td>
<td>118</td>
</tr>
<tr>
<td>Command Changes</td>
<td>119</td>
</tr>
<tr>
<td>Performance Indicator Changes</td>
<td>120</td>
</tr>
<tr>
<td>CSCuIj44396 - Support outlook application in P2P detection</td>
<td>121</td>
</tr>
<tr>
<td>Feature Changes</td>
<td>121</td>
</tr>
<tr>
<td>Command Changes</td>
<td>121</td>
</tr>
<tr>
<td>Performance Indicator Changes</td>
<td>122</td>
</tr>
<tr>
<td>CSCuI65264 - ADC Support for Badoo</td>
<td>123</td>
</tr>
<tr>
<td>Feature Changes</td>
<td>123</td>
</tr>
<tr>
<td>Command Changes</td>
<td>123</td>
</tr>
<tr>
<td>Performance Indicator Changes</td>
<td>124</td>
</tr>
<tr>
<td>CSCuI65272 - ADC Support Vine</td>
<td>125</td>
</tr>
<tr>
<td>Feature Changes</td>
<td>125</td>
</tr>
<tr>
<td>Command Changes</td>
<td>126</td>
</tr>
<tr>
<td>Performance Indicator Changes</td>
<td>127</td>
</tr>
<tr>
<td>CSCuIj82539 - Support for foursquare</td>
<td>128</td>
</tr>
<tr>
<td>Feature Changes</td>
<td>128</td>
</tr>
<tr>
<td>Command Changes</td>
<td>128</td>
</tr>
<tr>
<td>Performance Indicator Changes</td>
<td>129</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ADC Enhancements for September 30, 2013</th>
<th>131</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADC Feature Changes as of September 30, 2013</td>
<td>131</td>
</tr>
<tr>
<td>New ADC Features</td>
<td>131</td>
</tr>
<tr>
<td>Modified ADC Features</td>
<td>131</td>
</tr>
<tr>
<td>ADC Command Changes as of September 30, 2013</td>
<td>131</td>
</tr>
<tr>
<td>New ADC Commands</td>
<td>132</td>
</tr>
<tr>
<td>Modified ADC Commands</td>
<td>132</td>
</tr>
<tr>
<td>Deprecated ADC Commands</td>
<td>136</td>
</tr>
</tbody>
</table>
ADC Performance Indicator Changes as of September 30, 2013 ........................................... 136
New ADC Bulk Statistics .............................................................................................................. 136
Modified ADC Bulk Statistics ...................................................................................................... 136
 Deprecated ADC Bulk Statistics ................................................................................................... 136
New ADC Output Fields and Counters ......................................................................................... 136
Modified ADC Output Fields and Counters .................................................................................. 138
Deprecated ADC Output Fields and Counters ............................................................................. 138

ECS Changes in Release 15.0 ........................................................................................................ 139

ECS Enhancements for February 27, 2015 ................................................................................ 140
CSCus74979 - lower-ip-precedence not working when data packet exceeds CIR ....................... 140
Feature Changes .......................................................................................................................... 140

ECS Enhancements for October 31, 2014 ................................................................................ 141
CSCuo32161 - ASR5K: Need enhanced counters for QGR monitoring ....................................... 141
Feature Changes .......................................................................................................................... 141
Performance Indicator Changes .................................................................................................... 141
CSCup67356 - Rule failure counters not incremented ................................................................. 142
Feature Changes .......................................................................................................................... 142
Performance Indicator Changes .................................................................................................... 142
CSCuq15304 - Out-Of-Order timeout expires unexpectedly leading to misbilling ...................... 142
Feature Changes .......................................................................................................................... 142

ECS Enhancements for June 6, 2014 ........................................................................................ 143
CSCud41033 - flow idle timeout + flow limit for udp does not work ........................................... 143
Feature Changes .......................................................................................................................... 143

ECS Enhancements for April 15, 2014 ...................................................................................... 144
CSCuj77690 - Session Recovery Improvements for GGSN and PGW ....................................... 144
Feature Changes .......................................................................................................................... 144
CSCui61892 - Ran b/w optimization performed for flow-status other than DISABLED ............. 144
Feature Changes .......................................................................................................................... 144
CSCum91142 - PGW rejecting the rule modified by PCRF with QOS_Vidation failure ............. 145
Feature Changes .......................................................................................................................... 145
CSCun25302 - Rule failure handling: simultaneous change of eval pre & rule content ............. 145
Feature Changes .......................................................................................................................... 145

ECS Enhancements for March 31, 2014 .................................................................................... 146
CSCuj77690 - Session Recovery Improvements for GGSN and PGW ....................................... 146
Feature Changes .......................................................................................................................... 146
CSCui61892 - Ran b/w optimization performed for flow-status other than DISABLED ............. 146
Feature Changes .......................................................................................................................... 146
CSCum91142 - PGW rejecting the rule modified by PCRF with QOS_Vidation failure ............. 147
Feature Changes .......................................................................................................................... 147
CSCun25302 - Rule failure handling: simultaneous change of eval pre & rule content ............. 147
Feature Changes .......................................................................................................................... 147

ECS Enhancements for February 17, 2014 .............................................................................. 148
CSCui09884, CSCuf90188 - ECSV2 Volume Usage support post ICSR switchover ...................... 148
Feature Changes .......................................................................................................................... 148

ECS Enhancements for January 31, 2014 ............................................................................... 149
CSCui09884, CSCuf90188 - ECSV2 Volume Usage support post ICSR switchover ...................... 149
Feature Changes .......................................................................................................................... 149

ECS Enhancements for November 30, 2013 .......................................................................... 150
CSCub54839 - Full URL in EDR records .................................................................................... 150
Feature Changes .......................................................................................................................... 150
CSCuc32951 - EDRs to support User-Agent field greater than 128 bytes .................................. 150
Feature Changes .......................................................................................................................... 150
Command Changes ...................................................................................................................... 150
CSCui00558 - lte call gets terminated when default-eps-bearer-Qos modified in CCA-U .......................................................... 151
Feature Changes .......................................................................................................................... 151
CSCug37786 - Optimized Calculation of GBR MBR based on disabled flows .......................................................... 151
Feature Changes .......................................................................................................................... 152
Command Changes ...................................................................................................................... 152
Performance Indicator Changes ................................................................................................. 152
ECS Enhancements for September 30, 2013 .................................................................................. 153
ECS Feature Changes as of September 30, 2013 ........................................................................ 153
New ECS Features ....................................................................................................................... 153
Modified ECS Features .............................................................................................................. 156
ECS Command Changes as of September 30, 2013 .................................................................. 159
New ECS Commands .................................................................................................................. 159
Modified ECS Commands ......................................................................................................... 160
Deprecated ECS Commands ....................................................................................................... 160
ECS Performance Indicator Changes as of September 30, 2013 .............................................. 160
New ECS Bulk Statistics ............................................................................................................ 161
Modified ECS Bulk Statistics ...................................................................................................... 161
Deprecated ECS Bulk Statistics .................................................................................................. 161
New ECS Output Fields and Counters .......................................................................................... 161
Modified ECS Output Fields and Counters .................................................................................. 166
Deprecated ECS Output Fields and Counters ............................................................................ 167
ePDG Changes in Release 15.0 ..................................................................................................... 169
ePDG Enhancements for March 31, 2014 .................................................................................... 170
CSCum89534 - ePDG sends LVC traffic over S2b using default bearer not dedicated .................. 170
Feature Changes .......................................................................................................................... 170
Command Changes ..................................................................................................................... 170
ePDG Enhancements for November 30, 2013 ......................................................................... 172
CSCui62118 - [ePDG] - MAC Address extraction based on configured delimiter ......................... 172
Command Changes ..................................................................................................................... 172
username mac-address-delimiter .............................................................................................. 172
CSCui21539 - ePDG and HeNBGW combo .................................................................................. 173
Feature Changes .......................................................................................................................... 173
CSCui42954 - [ePDG] - MAC Address reporting to support @ AP_MAC_addr.nai NAI format ..... 173
Command Changes ..................................................................................................................... 173
ePDG Enhancements for September 30, 2013 ......................................................................... 175
ePDG Feature Changes as of September 30, 2013 .................................................................. 175
New ePDG Features ..................................................................................................................... 175
Modified ePDG Features ............................................................................................................. 175
Modified ePDG Commands ......................................................................................................... 176
ePDG Command Changes as of September 30, 2013 ............................................................... 177
New ePDG Commands ................................................................................................................ 177
Modified ePDG Commands ....................................................................................................... 178
Deprecated ePDG Commands .................................................................................................... 178
ePDG Performance Indicator Changes as of September 30, 2013 .......................................... 178
New ePDG Bulk Statistics .......................................................................................................... 178
Modified ePDG Bulk Statistics ................................................................................................... 178
Deprecated ePDG Bulk Statistics ............................................................................................... 179
New ePDG Output Fields and Counters ..................................................................................... 179
Modified ePDG Output Fields and Counters ............................................................................ 179
Deprecated ePDG Output Fields and Counters ........................................................................ 179
eWAG Changes in Release 15.0 ................................................................................................. 181
eWAG Enhancements for January 31, 2014 .............................................................................. 182
CSCuh44969 - eWAG support for multiple primary contexts .................................................. 182
Contents

GGSN Enhancements for January 31, 2014 .................................................. 182
GGSN Enhancements for February 27, 2015 ........................................... 182
eWAG Enhancements for November 30, 2013 ........................................ 182

Feature Changes .................................................................................. 182
Command Changes ............................................................................ 182
eWAG Enhancements for November 30, 2013 ........................................ 184
CSCub53946 - D-eWAG: eWAG to support Local Traffic breakout ........ 184
Feature Changes .............................................................................. 184
Performance Indicator Changes ........................................................... 185
CSCud96431 - D-eWAG: eWAG support on PSC3 cards ....................... 185
Feature Changes .............................................................................. 185
CSCue18931 - D-eWAG: Add Additional Radius AVP support For Local Break Out .......................................................... 185
Feature Changes .............................................................................. 185
CSCue63798 - D-eWAG: Support Radius Accounting for Local Breakout .......................................................... 186
Feature Changes .............................................................................. 186
eWAG Feature Changes as of September 30, 2013 ............................... 187
New eWAG Features .......................................................................... 187
R-eWAG Support for GGSN-initiated UPC ......................................... 187
R-eWAG Support for Local Configuration of GGSN IP Addresses .......... 187
R-eWAG Support for Alternate GGSN in Case Primary GGSN Rejects CPC .......................................................... 187
R-eWAG Support for CDR Functionality for Offline Charging ............ 188
R-eWAG Support for LI Functionality ............................................... 188
R-eWAG Support for Enhanced Failure Handling .............................. 188
eWAG Command Changes as of September 30, 2013 ......................... 189
New eWAG Commands .................................................................. 189
gtp peer-ip-address ........................................................................ 189
accounting-context ........................................................................ 189
Modified eWAG Commands ............................................................... 189
Deprecated eWAG Commands ............................................................ 190
ggsn-ip-address ............................................................................. 190
eWAG Performance Indicator Changes as of September 30, 2013 ........ 191

Firewall Changes in Release 15.0 ......................................................... 193

Firewall Enhancements for September 30, 2013 ................................. 194
Firewall Feature Changes as of September 30, 2013 ......................... 194
New Firewall Features ..................................................................... 194
Modified Firewall Features ............................................................... 194
Firewall Command Changes as of September 30, 2013 ...................... 195
New Firewall Commands ................................................................. 195
Modified Firewall Commands ............................................................ 196
Deprecated Firewall Commands ......................................................... 196
Firewall Performance Indicator Changes as of September 30, 2013 .... 196
New Firewall Bulk Statistics ............................................................. 197
Modified Firewall Bulk Statistics ....................................................... 197
Deprecated Firewall Bulk Statistics .................................................. 197
New Firewall Output Fields and Counters ........................................ 197
Modified Firewall Output Fields and Counters ................................... 199
Deprecated Firewall Output Fields and Counters ............................ 199

GGSN Changes in Release 15.0 ............................................................ 201

GGSN Enhancements for February 27, 2015 ...................................... 202
CSCun51617 - [gn-gp]: GGSN Not Informing PCRF about Network-Request-Support Change .................................................. 202
Feature Changes .............................................................................. 202
CSCur18773 - GGSN sends CPC resp of TEID all 0’s when newcall policy is configured .................................................. 203
Feature Changes .............................................................................. 203
GGSN Enhancements for January 31, 2014 ........................................ 204
CSCui12525 - BMC P-CSCF Discovery is not provided in CPC Response ........................................................................... 204
Feature Changes .............................................................................. 204

Cisco ASR 5x00 Release Change Reference
GTPP Changes in Release 15.0

GTPP Enhancements for April 30, 2014
- CSCu77461 - aaaproxy in warn state during call model run
  Feature Changes

GTPP Enhancements for January 31, 2014
- CSCy15478 - [GTP-SS]Gz: Cause to be 'Mngmnt-Intervntn' on clearing call from box
  Feature Changes

GTPP Enhancements for November 30, 2013
- CSCuf51057 - IPv6 Prefix
  Feature Changes

GTPP Enhancements for September 30, 2013
- GTPP Feature Changes
  New GTPP Features
  Modified GTPP Features

GTPP Command Changes
- New GTPP Commands
- Modified GTPP Commands

GGSN Changes in Release 15.0

GGSN Enhancements for November 30, 2013
- CSCu65167 - ASR5K ECS Shaping of multiple torrent downloads
  Feature Changes
- CSCu65556 - Sessmgr Crashes on seeing dhcpv6 server statistics
  Feature Changes
- CSCu89329 - (AlS)dpca-custom24: call dropped if Supported-feature AVP absent in CCR-I
  Feature Changes

GGSN Enhancements for April 30, 2014
- CSCu42540 - P-GW: DHCPv6 default UE prefix should be allocated from AAA and PD from DHCPv6
  Feature Changes
- CSCug55201: VZ BCPS QoS change; QCI<->MPLS EXP mapping for HA, UMTS-GGSN & eHRPD
  Feature Changes

GGSN Enhancements for September 30, 2013
- CSCuh73686 - GGSN: Modification of ‘timeout bearer-inactivity’ CLI to ignore default bearer
  Feature Changes

GGSN Performance Indicator Changes as of September 30, 2013
- CSCuh73686 - GGSN: Modification of ‘timeout bearer-inactivity’ CLI to ignore default bearer
  Command Changes

GGSN Command Changes as of September 30, 2013
- New GGSN Commands
- Modified GGSN Commands
- Deprecated GGSN Commands

GGSN Feature Changes as of September 30, 2013
- New GGSN Features
- Modified GGSN Features
- Deprecated GGSN Features

GGSN Bulk Statistics
- New GGSN Bulk Statistics
- Modified GGSN Bulk Statistics
- Deprecated GGSN Bulk Statistics

GGSN Output Fields and Counters
- New GGSN Output Fields and Counters
## HA Changes in Release 15.0

- HA Enhancements for September 30, 2013 ........................................ 238
- HA Feature Changes as of September 30, 2013 .................................. 238
- New HA Features .............................................................................. 238
- Modified HA Features ...................................................................... 238
- HA Command Changes as of September 30, 2013 ............................. 238
- HA Performance Indicator Changes as of September 30, 2013 ......... 238

## HNB-GW Changes in Release 15.0

- HNB-GW Enhancements for September 30, 2013 ............................. 240
- HNB-GW Feature Changes as of September 30, 2013 ....................... 240
- New HNB-GW Features .................................................................. 240
- Modified HNB-GW Features .............................................................. 241
- HNB-GW Command Changes as of September 30, 2013 ................. 241
- New HNB-GW Commands ............................................................... 241
- Modified HNB-GW Commands ........................................................ 243
- Deprecated HNB-GW Commands ...................................................... 243
- HNB-GW Performance Indicator Changes as of September 30, 2013 243
- New HNB-GW Bulk Statistics ............................................................ 243
- Modified HNB-GW Bulk Statistics .................................................... 243
- Deprecated HNB-GW Bulk Statistics ................................................. 243
- New HNB-GW Output Fields and Counters ....................................... 244
- Modified HNB-GW Output Fields and Counters .............................. 245
- Deprecated HNB-GW Output Fields and Counters ......................... 245

## HSGW Changes in Release 15.0

- HSGW Enhancements for October 31, 2014 .................................... 248
  - CSCuq05382 - Incorrect MNC_MCC in APN of PBU .......................... 248
    - Feature Changes ........................................................................ 248
- HSGW Enhancements for June 6, 2014 ............................................. 249
  - CSCun42462 - HSGW CLI to allow 0 value for reitres to Primary PGW 249
    - Feature Changes ...................................................................... 249
    - Command Changes .................................................................. 249
  - CSCuo16661 - IUBE Support on HSGW ........................................ 249
    - Feature Changes ...................................................................... 249
- HSGW Enhancements for November 30, 2013 ................................. 251
  - CSCuah39994 - Possible Memory Leak in sessctrl process observed in Customer CLAB setup .................................................. 251
    - Feature Changes ...................................................................... 251
- HSGW Enhancements for September 30, 2013 ................................ 252
- HSGW Feature Changes as of September 30, 2013 .......................... 252
  - New HSGW Features .................................................................. 252
  - Modified HSGW Features .............................................................. 253
CSCts36707 - IPSG qualification on ASR5500 (Ares) in IPSG Server Mode....................273
  Feature Changes ......................................................273
IPSG Enhancements for October 31, 2013 ................................................................274
  IPSG Feature Changes as of October 31, 2013 .........................................................274
  New IPSG Features ................................................................274
  Modified IPSG Features ........................................................274
IPSG Command Changes as of October 31, 2013 ......................................................274
IPSG Performance Indicator Changes as of October 31, 2013 .................................274
IPSG Enhancements for September 30, 2013 ..............................................................275
  IPSG Feature Changes as of September 30, 2013 ......................................................275
  New IPSG Features ................................................................275
  Modified IPSG Features ........................................................275
  IPSG Command Changes as of September 30, 2013 .................................................276
  New IPSG Commands ............................................................276
  Modified IPSG Commands ........................................................276
  Deprecated IPSG Commands .........................................................277
IPSG Performance Indicator Changes as of September 30, 2013 .............................278
  New IPSG Bulk Statistics ................................................................279
  Modified IPSG Bulk Statistics ................................................................279
  Deprecated IPSG Bulk Statistics ................................................................279
  New IPSG Output Fields and Counters .................................................................279
  Modified IPSG Output Fields and Counters .........................................................279
  Deprecated IPSG Output Fields and Counters .........................................................280
MME Changes in Release 15.0 ..................................................................................281
MME Enhancements for 15.0 MR6 ..........................................................................282
  CSCCuq88194 - New Reject cause needs to be added under Bearer Alloc Reject ESM message 282
  Feature Changes .................................................................282
  Performance Indicator Changes ..........................................................283
CSCur13994, CSCur89572 - ‘State/Location Information Retrieval’ flag support in Feature-list AVP 283
  Feature Changes .................................................................283
  Command Changes ................................................................284
  Performance Indicator Changes ..........................................................285
CSCur27407 - NewConnectionsDisallowed SNMP trap firing a lot ................................286
  Feature Changes .................................................................286
CSCur38243 - MME discards EGTP_CREATE_INDIRECT_DATA_FORWARDING_TUNNEL_RSP 287
  Feature Changes .................................................................287
CSCur50736 - PDN Connectivity Reject : Incorrect ESM cause#27 ............................287
  Feature Changes .................................................................287
  Command Changes .................................................................287
  Performance Indicator Changes ..........................................................288
CSCur89996 - MME releases UE context with Category NAS : Unspecified for Radio issues 289
  Feature Changes .................................................................289
  Command Changes ................................................................289
CSCur97956, CSCun97512 - Enabling Paging Optimization ........................................290
  Feature Changes .................................................................290
  Command Changes ................................................................290
CSCus00927 - S1 and SGs associations not equally distributed across mmemgr tasks 291
  Feature Changes .................................................................291
  Command Changes ................................................................291
  Performance Indicator Changes ..........................................................292
CSCus14148 - Dynamic Paging cache size allocation through CLI ..............................293
  Feature Changes .................................................................293
  Command Changes ................................................................293
CSCus25950 - [VoLTE] After IDR of T-ADS for Volte, MME modifies QoS of APN ........294
Feature Changes .................................................................................. 294
CSCu142726 - QoS : Incorrect Reliability Class Mapping from QCI=5 ....... 294
Feature Changes ............................................................................. 294
MME Enhancements for September 30, 2014 ..................................... 295
CSCu142726 - CxGW - show subscribers sgw-address <IP> not working as expected .................................................. 295
Command Changes ........................................................................ 295
CSCu69493 - MME - call-control-profile qos ue-ambr prefer-as-cap problems .......................................................... 296
Feature Changes ............................................................................. 296
CSCu17932 - MME sending old QoS values to UE after HO from 2G>4G>2G ................................................................. 296
Feature Changes ............................................................................. 296
Command Changes ........................................................................ 296
Performance Indicator Changes ......................................................... 297
CSCuo27283 - Roaming QoS Control .................................................. 297
Feature Changes ............................................................................. 297
Command Changes ........................................................................ 298
Performance Indicator Changes ......................................................... 299
CSCup23821 - NPUMGR Restart causing MME enB SCTP failures and impact to SGs/S1AP .................................................... 299
Feature Changes ............................................................................. 299
Performance Indicator Changes ......................................................... 300
CSCup29345 - Need MMEmgr CPU and Memory bulkstat counter for MME capacity monitoring ........................................... 301
Feature Changes ............................................................................. 301
Performance Indicator Changes ......................................................... 301
CSCup54025 - S1 and SGs associations not equally distributed across mmemgr tasks ......................................................... 301
Feature Changes ............................................................................. 301
Performance Indicator Changes ......................................................... 302
CSCup67478 - Reset-Req delete all sessions and send wrong feature-list to other HSSs ......................................................... 302
Feature Changes ............................................................................. 302
CSCup71470 - Not interpreting RZC H6a AVP as a full hexadecimal value ................................................................. 302
Feature Changes ............................................................................. 302
Command Changes ........................................................................ 303
Performance Indicator Changes ......................................................... 303
CSCuq142726 - Low S1 signalling and low response for TAU requests ................................................................. 304
Feature Changes ............................................................................. 304
CSCuq142726 - MME-CSFB: Handling of CSFB procedure for ongoing handover ......................................................... 304
Feature Changes ............................................................................. 304
CSCuq74468 - MME TAU release cause with ESM failure when PGW is not responding .................................................. 304
Feature Changes ............................................................................. 304
Command Changes ........................................................................ 305
Performance Indicator Changes ......................................................... 306
CSCuq86036 - Incorrect CLI text against Default bearer qos in ............. 307
Performance Indicator Changes ......................................................... 307
MME Enhancements for June 6, 2014 ................................................. 308
CSCts21153 - Change bulkstats variable for Retransmitted SCTP data chunks ............................................................. 308
Performance Indicator Changes ......................................................... 308
CSCuh22222 - Allow the MME to construct the Destination Realm from the MNC/MCC ..................................................... 309
Feature Changes ............................................................................. 309
Command Changes ........................................................................ 309
Performance Indicator Changes ......................................................... 310
CSCum83308 - MME Support for SGs Cause Code Mapping ............... 310
Feature Changes ............................................................................. 310
Command Changes ........................................................................ 310
Performance Indicator Changes ......................................................... 310
CSCun94236 - MME uses wrong sec keys during 3g to 4g IRAT leading to SOS ............................................................. 311
Feature Changes ............................................................................. 311
CSCuo45960 - If both ipv4 & ipv6 GGSN addr available, MME to fwd ipv4 addr to SGSN ..................................311
Feature Changes .................................................................................................................................311
Performance Indicator Changes ...........................................................................................................312
MME Enhancements for March 31, 2014 .................................................................................................313
CSCun23099 - STN-SR IE encoding is incorrect on Sv interface ..............................................................313
Feature Changes .................................................................................................................................313
Command Changes .............................................................................................................................314
Performance Indicator Changes ...........................................................................................................314
CSCun28592 - S6a Feature List AVP is hardcoded in MME .................................................................314
Feature Changes .................................................................................................................................314
MME Enhancements for January 31, 2014 ...............................................................................................315
CSCud33786 - GnGp: sgtpc: Incoming RIM messages are not sent to target enodeB ...............................315
Feature Changes .................................................................................................................................315
CSCug78485, CSCuj28520, CSCuj28539 - EMM/ESM Cause Codes in in bulkstats/counters ..................316
Performance Indicator Changes ...........................................................................................................316
CSCuj49578 - scpt link not established with scpt-sack-period 0 in scpt-param-template .......................321
Feature Changes .................................................................................................................................321
CSCuj77490 - MME Incomplete Suspend Response towards SGSN via Gn (gtp-c v1) ..............................321
Feature Changes .................................................................................................................................321
CSCui43064 - IE 95/94 should not be included in case X2HO w/out SGW change .........................321
Feature Changes .................................................................................................................................321
CSCub06765 - Overcharging protection ...............................................................................................322
Feature Changes .................................................................................................................................322
Command Changes .............................................................................................................................322
Performance Indicator Changes ...........................................................................................................323
MME Enhancements for November 30, 2013 ......................................................................................324
CSCui50770 - NW Shared mme allocating wrong plmn in GUTI during TAU after 3g/4g srns .............324
Feature Changes .................................................................................................................................324
MME Enhancements for September 30, 2013 .....................................................................................326
MME Feature Changes as of September 30, 2013 ..................................................................................326
New MME Features ..............................................................................................................................326
Modified MME Features .......................................................................................................................327
MME Command Changes as of September 30, 2013 .........................................................................332
New MME Commands .........................................................................................................................332
Modified MME Commands ..................................................................................................................336
Deprecated MME Commands ...............................................................................................................341
MME Performance Indicator Changes as of September 30, 2013 .....................................................341
New MME Bulk Statistics .....................................................................................................................341
Modified MME Bulk Statistics .............................................................................................................344
Deprecated MME Bulk Statistics ..........................................................................................................344
New MME Output Fields and Counters ...............................................................................................345
Modified MME Output Fields and Counters .........................................................................................349
Deprecated MME Output Fields and Counters ....................................................................................350

MVG Changes in Release 15.0.........................................................................................................................351
MVG Enhancements for September 30, 2013 .....................................................................................352
MVG Feature Changes as of September 30, 2013 .................................................................................352
New MVG Features ...............................................................................................................................352
Modified MVG Features .......................................................................................................................353
MVG Command Changes as of September 30, 2013 .........................................................................354
New MVG Commands ..........................................................................................................................354
Modified MVG Commands ..................................................................................................................354
Deprecated MVG Commands ...............................................................................................................354
MVG Performance Indicator Changes as of September 30, 2013 .....................................................354
New MVG Bulk Statistics ......................................................................................................................355
PDSN Changes in Release 15.0 .............................................................................. 359
  NAT Changes in Release 15.0 .............................................................................. 359
  NAT Enhancements for September 30, 2013 .................................................. 360
  NAT Feature Changes as of September 30, 2013 ........................................... 360
  New NAT Features ......................................................................................... 360
  Modified NAT Features ................................................................................ 360
  NAT Command Changes as of September 30, 2013 ..................................... 361
  New NAT Commands .................................................................................... 361
  Modified NAT Commands ............................................................................ 362
  Deprecated NAT Commands ........................................................................ 363
  NAT Performance Indicator Changes as of September 30, 2013 .................... 363
  New NAT Bulk Statistics ............................................................................... 363
  Modified NAT Bulk Statistics ....................................................................... 364
  Deprecated NAT Bulk Statistics ................................................................... 364
  New NAT Output Fields and Counters .......................................................... 364
  Modified NAT Output Fields and Counters .................................................. 365
  Deprecated NAT Output Fields and Counters .............................................. 366

PDSN Changes in Release 15.0 .............................................................................. 367
  PDSN Enhancements for February 27, 2015 ................................................... 368
  CSCus41228 - PDSN not to terminate PPP session when handoff within a restricted zone ........................................................................................................ 368
  Feature Changes ............................................................................................ 368
  CSCus51341 - [L2TP] ICRQ to include IMSI based on config CLI .................... 369
  Feature Changes ............................................................................................ 369
  Command Changes ........................................................................................ 369
  PDSN Enhancements for October 31, 2014 ...................................................... 370
  CSCup93612 - PDSN support for enhanced PPP Redirection ............................ 370
  Feature Changes ............................................................................................ 370
  Command Changes ........................................................................................ 371
  PDSN Enhancements for April 10, 2014 ........................................................... 372
  CSCun65435 - Assertion at sessmgr_imsa.c:453 Function: sessmgr_authorize_with_imsa() ......................................................................................... 372
  Feature Changes ............................................................................................ 372
  PDSN Enhancements for Jan 31, 2014 .............................................................. 373
  CSCud89827 - PCF-wise bulkstats & reports .................................................. 373
  Feature Changes ............................................................................................ 373
  Performance Indicator Changes ...................................................................... 373
  CSCue70505 - Add PCF as an Index in PPP and RP Schemas ............................ 375
  Feature Changes ............................................................................................ 375
  Performance Indicator Changes ...................................................................... 375
  PDSN Enhancements for November 30, 2013 ................................................ 377
  CSCuj49921 - IP Pool Group bulkstat variables show individual pool stats .... 377
  Feature Changes ............................................................................................ 377
  Performance Indicator Changes ...................................................................... 377
  PDSN Enhancements for September 30, 2013 ................................................. 379
  PDSN Feature Changes as of September 30, 2013 ......................................... 379
  New PDSN Features ....................................................................................... 379
  Modified PDSN Features .............................................................................. 379
  PDSN Command Changes as of September 30, 2013 .................................... 379
  PDSN Performance Indicator Changes as of September 30, 2013 ................. 379
P-GW Changes in Release 15.0 .......................................................... 381

P-GW Enhancements for February 27, 2015 ........................................... 382
CSCuc76443 - Wrong IE in PDP response to PDP context without TFT already activated .......................... 382
Feature Changes ........................................................................... 382
CPC Reject Reason ......................................................................... 382
P-GW Enhancements for October 31, 2014 .............................................. 383
CSCui10427 - default behavior for vrf-multipath is to use the global multipath ............................................. 383
Feature Changes ........................................................................... 383
CSCuo06912 - PGW call fails if Framed-Pool enforced from radius ................................................................. 384
Feature Changes ........................................................................... 384
CSCuo95038 - PGW forces lower AMBR values than received .......................................................................... 384
Feature Changes ........................................................................... 384
CSCuq39165 - [OCS FOA] Create Session Response is not sent out from PGW ..................................................... 384
Feature Changes ........................................................................... 384
P-GW Enhancements for January 31, 2014 .............................................. 385
CSCug69032 - if v6 pcscf address is not available, ip name-server addresses are sent ........................................ 385
Feature Changes ........................................................................... 385
CSCuh28006, CSCui24601 - Additional application support with DSCP-802.1p Marking per Interface .............. 386
Feature Changes ........................................................................... 386
Command Changes ........................................................................ 386
Performance Indicator Changes .......................................................... 386
CSCui91396 - egtpmgr 143137 info GTP-C path failure egtpmgr on Standby ......................................................... 388
Feature Changes ........................................................................... 388
CSCui24817 - Change in the 802.1p/MPLS-EXP configuration in QCI table ......................................................... 388
Feature Changes ........................................................................... 388
Command Changes ........................................................................ 388
Performance Indicator Changes .......................................................... 388
CSCui65556 - Sessmgr Crashes on seeing dhcpv6 server statistics ..................................................................... 390
Feature Changes ........................................................................... 390
CSCui93209 - Need show config errors to point inconsistencies in qos configuration ....................................... 390
Performance Indicator Changes .......................................................... 390
P-GW Enhancements for November 30, 2013 ......................................... 392
CSCui65085 - CxGW:Wrong update of ULI to PCRF during idle tau w/o mme/sgw relocation ......................... 392
Feature Changes ........................................................................... 392
CSCui80818 - Enhancement to have the delta route modifier for SRP systems ASR5X ........................................ 393
Feature Changes ........................................................................... 393
Command Changes ........................................................................ 393
CSCuh66364 - Acct-Termination-Cause in acct stop msg shows Unknown SRVCC PS to CS HO393
Feature Changes ........................................................................... 393
CSCuh71681 - END_USER_IMSI value received on S6b is reported as END_USER_E164 onGy,Rf394
Feature Changes ........................................................................... 394
CSCuh73686, CSCui49747 - P-GW: Modification of ‘timeout bearer-inactivity’ CLI to ignore default bearer 394
CommandChanges ........................................................................ 394
CSCui42540 - P-GW: DHCPv6 default UE prefix should be allocated from AAA and PD from DHCPv6 395
FeatureChanges ............................................................................ 395
CSCui47287 - AAA radius returned ip address should be dynamic for PGW ....................................................... 395
FeatureChanges ............................................................................ 395
CSCui98507 - Call loss when SGW restoration with same SGW in progress ......................................................... 396
FeatureChanges ............................................................................ 396
CSCui23543 - PGW rejects session with Status as Adminiprohibited in PMIP PBA .............................................. 396
FeatureChanges ............................................................................ 396
P-GW Enhancements for October 30, 2013 .............................................. 397
P-GW Feature Changes as of October 30, 2013 ....................................... 397
New P-GW Features........................................................................................................ 397
Modified P-GW Features ............................................................................................... 397
P-GW Command Changes as of October 30, 2013....................................................... 397
P-GW Performance Indicator Changes as of October 30, 2013................................. 397
P-GW Enhancements for September 30, 2013.............................................................. 398
P-GW Feature Changes as of September 30, 2013 ...................................................... 398
New P-GW Features ...................................................................................................... 398
Modified P-GW Features ............................................................................................... 403
P-GW Command Changes as of September 30, 2013................................................... 412
New P-GW Commands ................................................................................................... 412
Modified P-GW Commands ......................................................................................... 416
Deprecated P-GW Commands ...................................................................................... 421
P-GW Performance Indicator Changes as of September 30, 2013.............................. 421
New P-GW Bulk Statistics ............................................................................................. 421
Modified P-GW Bulk Statistics ..................................................................................... 429
Deprecated P-GW Bulk Statistics ................................................................................. 429
New P-GW Output Fields and Counters ...................................................................... 429
Modified P-GW Output Fields and Counters ................................................................. 434
Deprecated P-GW Output Fields and Counters ............................................................. 434

SAEGW Changes in Release 15.0 ................................................................................ 435

SAEGW Enhancements for February 27, 2015 ............................................................. 436
SAEGW Enhancements for October 31, 2014 .............................................................. 437
CSCUn35216 - S4 to Gn SGSN HO, CCR-u shows RAT type event for UTRAN .......... 437
  Feature Changes ........................................................................................................ 437
CSCUp67356 - Rule failure counters not incremented ................................................. 438
  Feature Changes ........................................................................................................ 438
CSCuq25059 - Assertion failure at sess/smgr/sessmgr_ggsn.c:25058 ......................... 438
  Feature Changes ........................................................................................................ 438
SAEGW Enhancements for November 30, 2013 ........................................................ 439
CSCui79823 - Customer ENT LAB- Tracfone local issue for iRat from 4G to S4 ........... 439
  Feature Changes ........................................................................................................ 439
SAEGW Enhancements for September 30, 2013 ........................................................ 441
SAEGW Feature Changes as of September 30, 2013 ............................................... 441
  New SAEGW Features ............................................................................................... 441
  Modified SAEGW Features ...................................................................................... 441
SAEGW Command Changes as of September 30, 2013 ............................................. 443
  New SAEGW Commands .......................................................................................... 443
  Modified SAEGW Commands ............................................................................... 445
  Deprecated SAEGW Commands .............................................................................. 446
SAEGW Performance Indicator Changes as of September 30, 2013......................... 446
  New SAEGW Bulk Statistics ..................................................................................... 446
  Modified SAEGW Bulk Statistics .......................................................................... 459
  Deprecated SAEGW Bulk Statistics ....................................................................... 459
  New SAEGW Output Fields and Counters ............................................................... 459
  Modified SAEGW Output Fields and Counters ...................................................... 460
  Deprecated SAEGW Output Fields and Counters ................................................. 460

SGSN Changes in Release 15.0 .................................................................................. 463

SGSN Enhancements for 15.0 MR6 ............................................................................. 464
CSCur29374 - Service reject GMM casue 101 causing Service request loop ............... 464
  Feature Changes ....................................................................................................... 464
CSCur74184 - Global CN-ID should be sent in DirectInformationTransfer RIM with iuflex 465
  Feature Changes ....................................................................................................... 465
<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCul04175</td>
<td>S4-SGSN to support R11 agreed CR to avoid SRVCC race condition</td>
</tr>
<tr>
<td>Command Changes</td>
<td></td>
</tr>
<tr>
<td>CSCuo56840</td>
<td>'authenticate activate' not working for 3G calls</td>
</tr>
<tr>
<td>Feature Changes</td>
<td></td>
</tr>
<tr>
<td>CSCuo86321</td>
<td>issue with show subscriber and clear subscriber</td>
</tr>
<tr>
<td>Feature Changes</td>
<td></td>
</tr>
<tr>
<td>CSCuo93431</td>
<td>PDP failure due to subscribers stuck in disconnecting state</td>
</tr>
<tr>
<td>Feature Changes</td>
<td></td>
</tr>
<tr>
<td>CSCup14871</td>
<td>Addition of logs/stats to analyze the call distribution issue</td>
</tr>
<tr>
<td>Feature Changes</td>
<td></td>
</tr>
<tr>
<td>CSCup23087, CSCup94308</td>
<td>Assertion failure with Invalid/unhandled event PMM_EVT_SM_INC_HO_COMP</td>
</tr>
<tr>
<td>Feature Changes</td>
<td></td>
</tr>
<tr>
<td>CSCup34047</td>
<td>Additional checks/logs to find the trigger for Wrong DNS query</td>
</tr>
<tr>
<td>Feature Changes</td>
<td></td>
</tr>
<tr>
<td>CSCup34085</td>
<td>Sgtpmcmgr high ErrIn may cause rx drop and path failure after demux migration</td>
</tr>
<tr>
<td>Feature Changes</td>
<td></td>
</tr>
<tr>
<td>CSCup4785, CSCup34454</td>
<td>QOS management for uplink data messages in 2G</td>
</tr>
<tr>
<td>Feature Changes</td>
<td></td>
</tr>
<tr>
<td>CSCup94835</td>
<td>SGSM/MME :PC: [0aae198f/X] client_bounce()</td>
</tr>
<tr>
<td>Feature Changes</td>
<td></td>
</tr>
<tr>
<td>CSCui25521</td>
<td>show service all provides incorrect values</td>
</tr>
<tr>
<td>Feature Changes</td>
<td></td>
</tr>
<tr>
<td>CSCul62285</td>
<td>IP tcp mss settings on sgsn</td>
</tr>
<tr>
<td>Feature Changes</td>
<td></td>
</tr>
<tr>
<td>CSCul70235</td>
<td>'show sgsn sessmgr all ptmsi statistics' displays NRI Values incorrectly</td>
</tr>
<tr>
<td>Feature Changes</td>
<td></td>
</tr>
<tr>
<td>CSCun89264, CSCui65387</td>
<td>[RIM] : Enhancements to Handling subsequent rim segments</td>
</tr>
<tr>
<td>Feature Changes</td>
<td></td>
</tr>
<tr>
<td>CSCuo62754</td>
<td>Assertion failure at sess/sgsn/sgsn-app/db/sgsn_db_pmm.c:1880</td>
</tr>
<tr>
<td>Feature Changes</td>
<td></td>
</tr>
<tr>
<td>CSCul55835</td>
<td>qos-dscp no cs3 mode unavailable</td>
</tr>
</tbody>
</table>

**Contents**

SGSN Enhancements for October 31, 2014 ......................................................... 466
CSCul04175 - S4-SGSN to support R11 agreed CR to avoid SRVCC race condition 466
Command Changes ................................................................. 466
CSCuo56840 - 'authenticate activate' not working for 3G calls ......................... 467
Feature Changes ................................................................. 467
Command Changes ................................................................. 467
Performance Indicator Changes .................................................. 467
CSCuo86321 - issue with show subscriber and clear subscriber ........................ 468
Feature Changes ................................................................. 468
CSCuo93431 - PDP failure due to subscribers stuck in disconnecting state .......... 468
Feature Changes ................................................................. 468
CSCup14871 - Addition of logs/stats to analyze the call distribution issue .......... 469
Feature Changes ................................................................. 469
CSCup23087, CSCup94308 - Assertion failure with Invalid/unhandled event PMM_EVT_SM_INC_HO_COMP 469
Feature Changes ................................................................. 469
Command Changes ................................................................. 469
Performance Indicator Changes .................................................. 470
CSCup34047 - Additional checks/logs to find the trigger for Wrong DNS query 470
Feature Changes ................................................................. 470
CSCup34085 - Sgtpmcmgr high ErrIn may cause rx drop and path failure after demux migration 471
Feature Changes ................................................................. 471
Command Changes ................................................................. 471
Performance Indicator Changes .................................................. 472
CSCup4785, CSCup34454 - QOS management for uplink data messages in 2G .......... 473
Feature Changes ................................................................. 473
CSCup94835 - SGSM/MME :PC: [0aae198f/X] client_bounce() ......................... 475
Feature Changes ................................................................. 475
Command Changes ................................................................. 475
SGSN Enhancements for June 6, 2014 ......................................................... 476
CSCul25521 - show service all provides incorrect values ............................ 476
Feature Changes ................................................................. 476
CSCul62285 - IP tcp mss settings on sgsn .............................................. 477
Feature Changes ................................................................. 477
Command Changes ................................................................. 477
CSCul70235 - 'show sgsn sessmgr all ptmsi statistics' displays NRI Values incorrectly 477
Feature Changes ................................................................. 477
CSCun89264, CSCui65387 - [RIM] : Enhancements to Handling subsequent rim segments 478
Feature Changes ................................................................. 478
Performance Indicator Changes .................................................. 478
CSCuo62754 - Assertion failure at sess/sgsn/sgsn-app/db/sgsn_db_pmm.c:1880 479
Feature Changes ................................................................. 479
SGSN Enhancements for April 10, 2014 ...................................................... 480
CSCui65387, CSCun89264 - [RIM] : Enhancements to Handling subsequent rim segments 480
Feature Changes ................................................................. 480
Performance Indicator Changes .................................................. 481
SGSN Enhancements for March 31, 2014 ...................................................... 482
CSCtz55422 - SGSN should start dns query for default SGSN when nri based query fails 482
Feature Changes ................................................................. 482
Command Changes ................................................................. 483
CSCuh86390 - [2G-MOCN]Counters for redirection complete sent in retry messages 483
Feature Changes ................................................................. 483
Performance Indicator Changes .................................................. 483
CSCui55835 - qos-dscp no cs3 mode unavailable ..................................... 484
Command Changes ........................................................................................................ 484
CSCum03845 - LTE to 3G IRAT-idle mode failed due to missing RNC TEID in EGTP_UBR .... 484
Feature Changes ........................................................................................................... 484
Command Changes ........................................................................................................ 484
Performance Indicator Changes ...................................................................................... 485
CSCum52817 - Do Not establish RAB even if ASI bit is set ........................................... 485
Feature Changes ........................................................................................................... 485
Command Changes ........................................................................................................ 486
Performance Indicator Changes ...................................................................................... 486
CSCum56947 - Configuration to enable sending extended MBR for UL/DL ................. 486
Feature Changes ........................................................................................................... 486
Command Changes ........................................................................................................ 487
CSCum56967 - Security Issue - Encryption on MME/SGSN level ............................... 487
Feature Changes ........................................................................................................... 487
Command Changes ........................................................................................................ 488
Performance Indicator Changes ...................................................................................... 488
CSCum62465 - SGSN hangs and lots of Assertion failure at snutil/sn_memblock.c:188 .... 489
Feature Changes ........................................................................................................... 489
Performance Indicator Changes ...................................................................................... 489
CSCum76067 - GMM-T3323 Timeout display some junk value under sgsn-service .... 489
Feature Changes ........................................................................................................... 489
CSCun09183 - SGSN should not cleanup the subscriber when XID exchange times out .. 489
Feature Changes ........................................................................................................... 489
CSCun13033 - Detach request is not triggered in following scenario ......................... 490
Feature Changes ........................................................................................................... 490
SGSN Enhancements for January 31, 2014 ........................................................................ 491
CSCue50555 - S-CDR should quantify the volume drop with probable cause code/counter 491
Feature Changes ........................................................................................................... 491
CSCui42601 - Require Intra-SRNS and Inter-SRNS bulkstat counter ......................... 492
Performance Indicator Changes ...................................................................................... 492
CSCuj28230 - Additional specific 2G/3G counters for SGSN ....................................... 493
Performance Indicator Changes ...................................................................................... 493
CSCuj73484 - GPRS MOCN: Bulkstats to be added for counters ............................... 494
Performance Indicator Changes ...................................................................................... 494
CSCuj73688 - EMS support required for new counters in SGSN gmm-sm Statistics .... 495
Feature Changes ........................................................................................................... 495
SGSN Enhancements for November 30, 2013 ............................................................. 496
CSCua59413 - SGSN support required to route Direct InformationTransfer msg to eNB 496
Feature Changes ........................................................................................................... 496
CSCue89610 - [15.0] Route to remote PC via linkset not removed on deletion of linkset 497
Feature Changes ........................................................................................................... 497
CSCuh34564 - IDT in 2g should be supported for both Gn and S4 SGSN .................... 497
Feature Changes ........................................................................................................... 497
CSCuh99198 - CLI config to Accept RAB negotiation for PDP Activation in S4-SGSN 498
Feature Changes ........................................................................................................... 498
Command Changes ........................................................................................................ 498
Performance Indicator Changes ...................................................................................... 499
CSCui65204 - [EDR]: SNMP trap not generating after EDR file deletion .................... 499
Feature Changes ........................................................................................................... 499
CSCuj13922 - Text string is not displayed properly in GMM INFO msg in this scenario 499
Feature Changes ........................................................................................................... 499
SGSN Enhancements for September 30, 2013 ............................................................. 501
SGSN Feature Changes as of September 30, 2013 ....................................................... 501
New SGSN Features ....................................................................................................... 501
Contents

SNMP MIB Alarm Changes as of October 31, 2014 ................................................................. 575
New SNMP MIB Alarms ................................................................................................. 575
Modified SNMP MIB Alarms .................................................................................. 575
Deprecated SNMP MIB Alarms ............................................................................. 575

S-GW Changes in Release 15.0 ....................................................................................... 543
S-GW Enhancements for February 27, 2015 ................................................................. 544
CSCur53899 - instance 5 should be sent in UL IDFT rsp from s.sgw to s.mme .......... 544
Feature Changes ........................................................................................................ 544

S-GW Enhancements for March 30, 2014 ................................................................. 546
CSCum63316 - SGW responds with Man. IE incorrect sent by Target SGSN (HO Testing) ................................................................. 546
Feature Changes ........................................................................................................ 546
CSCum65866 - cli required to control pgw fileid in relocation create session response. 547
Feature Changes ........................................................................................................ 547

S-GW Enhancements for September 30, 2013 .............................................................. 549
CSCui75767 - SGW full checkpoint to micro checkpoint conversion - Phase 1 .... 549
Feature Changes ........................................................................................................ 549

S-GW Feature Changes as of September 30, 2013 ..................................................... 551
New S-GW Features .................................................................................................... 551
Modified S-GW Features ............................................................................................ 553

S-GW Command Changes as of September 30, 2013 ................................................ 557
New S-GW Commands ............................................................................................... 557
Modified S-GW Commands ..................................................................................... 559
Deprecated S-GW Commands ................................................................................. 559

S-GW Performance Indicator Changes as of September 30, 2013 ......................... 563
New S-GW Bulk Statistics ......................................................................................... 563
Modified S-GW Bulk Statistics ............................................................................... 567
Deprecated S-GW Bulk Statistics ............................................................................. 567
New S-GW Output Fields and Counters .................................................................. 567
Modified S-GW Output Fields and Counters ............................................................ 567
Deprecated S-GW Output Fields and Counters ......................................................... 567

SNMP MIB Changes in Release 15.0 ............................................................................. 573
SNMP MIB Object Changes as of October 31, 2014 .................................................. 574
New SNMP MIB Objects ............................................................................................ 574
Modified SNMP MIB Objects ................................................................................... 574
Deprecated SNMP MIB Objects ............................................................................... 574

SNMP MIB Alarm Changes as of October 31, 2014 .................................................. 575
New SNMP MIB Alarms ............................................................................................ 575
Modified SNMP MIB Alarms ................................................................................... 575
Deprecated SNMP MIB Alarms ............................................................................... 575
System Changes in Release 15.0 ................................................................. 591
System and Platform Enhancements for October 31, 2014 .......................... 592
CSCuo84268 - show etgpc peers needs to be added to the SSD ................... 592
  Feature Changes .................................................................................. 592
  Performance Indicator Changes ............................................................ 592
System and Platform Enhancements for February 17, 2014 ........................ 593
CSCui80584 - rem_addr is not being sent by the ASR to ACS ...................... 593
  Feature Changes .................................................................................. 593
  Command Changes .............................................................................. 593
System and Platform Enhancements for January 31, 2014 .......................... 595
CSCui80584 - rem_addr is not being sent by the ASR to ACS ...................... 595
  Feature Changes .................................................................................. 595
  Command Changes .............................................................................. 595
System and Platform Enhancements for November 30, 2013 ...................... 597
## System and Platform Enhancements

**For October 30, 2013**

- System Feature Changes
  - New System Features
  - Modified System Features

- System Command Changes
  - New System Commands
  - Modified System Commands
  - Deprecated System Commands

- System Performance Indicator Changes
  - New System Bulk Statistics
  - Modified System Bulk Statistics
  - Deprecated System Bulk Statistics
  - New System Output Fields and Counters
  - Modified System Output Fields and Counters
  - Deprecated System Output Fields and Counters

- System Security Management Changes
  - New System Security Commands
  - Modified System Security Commands
  - Deprecated System Security Commands

---

### Web Element Manager Changes in Release 15.0

**Enhancements for April 30, 2014**

- CSCui68311 - EMS support required new counter "Paging Dropped" in MME S1AP Statistics
- CSCui68315 - EMS support required for newly added Intra-SRNS and Inter-SRNS bulk-stat
- CSCum20624 - EMS support required for the new bulkstats added for CSCui71700
- CSCum26182 - WEM Support for luru F2F feature for HNBGW
- CSCum54746 - [BS Config]: &quot;Syst Local File Storage&quot; configurable is removed from CLI
- CSCum73297 - [BS] Counters not supported in WEM

---

<table>
<thead>
<tr>
<th>Feature Changes</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCue00484</td>
<td>597</td>
</tr>
<tr>
<td>CSCui34979</td>
<td>597</td>
</tr>
<tr>
<td>CSCui52107</td>
<td>597</td>
</tr>
<tr>
<td>CSCui75677</td>
<td>598</td>
</tr>
<tr>
<td>CSCui91943</td>
<td>598</td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>System Feature Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 30, 2013</td>
</tr>
<tr>
<td>System Performance Indicator Changes</td>
</tr>
<tr>
<td>October 30, 2013</td>
</tr>
<tr>
<td>System Security Management Changes</td>
</tr>
<tr>
<td>October 30, 2013</td>
</tr>
</tbody>
</table>
CSCum80541 - WEM 15.0.2304 - GUI not showing 15.0 ASR5x00 crash data correctly........633
  Feature Changes ........................................................................................................633
CSCun22514 - Bulk statistics support for ASR5K R16 ..................................................634
  Feature Changes ........................................................................................................634
Performance Indicator Changes ..................................................................................634
CSCun24706 - Alarm support for ASR5K R16 ...............................................................653
  Feature Changes ........................................................................................................653
WEM Enhancements for Jan 31, 2014 ........................................................................654
CSCue70505 - Add PCF as an Index in PPP and RP Schemas .......................................654
  Feature Changes ........................................................................................................654
Performance Indicator Changes ..................................................................................654
CSCui90658 - KT EPC : SGW - UDPC : Support required for UDPC UMIO and DPC(R02) in WEM655
  Feature Changes ........................................................................................................655
CSCuj14134 - Support required for new BS counters in 15.0 ......................................656
  Feature Changes ........................................................................................................656
Performance Indicator Changes ..................................................................................656
CSCui37079 - TW APTG-WEM server: PCFUnreachable NOT auto cleared - 15.0.2304 675
  Feature Changes ........................................................................................................675
WEM Enhancements for September 30, 2013 ..............................................................676
WEM Feature Changes as of September 30, 2013 .....................................................676
  New WEM Features .....................................................................................................676
Modified WEM Features ............................................................................................676
WEM Fault Management Changes as of September 30, 2013 ................................677
WEM Configuration Management Changes as of September 30, 2013 ....................678
WEM Accounting Management Changes as of September 30, 2013 .....................678
WEM Performance Management Changes as of September 30, 2013 .......................678
About this Guide

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

This book includes new feature descriptions and configuration, performance, and security changes for the 15.0 release. The Release Change Reference is separated into individual chapters per product and also includes chapters for system-level, SNMP MIB, and accounting management changes. Each chapter is also separated into sections that indicate the changes to the product documentation sorted by the date that this change was included in the product documentation.

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

The following tables describe the conventions used throughout this documentation.

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

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

Related Documentation

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

The following common documents are available:

- Hardware Installation Guide (hardware dependent)
- System Administration Guide (hardware dependent)
- Command Line Interface Reference
- Product Administration Guide (product specific)
- AAA Interface Administration Reference
- GTPP Interface Administration Reference
- Product Overview
- Statistics and Counters Reference
- Thresholding Configuration Guide

Obtaining Documentation

The most current Cisco documentation is available on the following website:

http://www.cisco.com/cisco/web/psa/default.html
Contacting Customer Support

Use the information in this section to contact customer support.

Refer to the support area of http://www.cisco.com for up-to-date product documentation or to submit a service request. A valid username and password are required to access this site. Please contact your Cisco sales or service representative for additional information.
Chapter 1
AAA Changes in Release 15.0

This chapter identifies accounting management features and functionality added to, modified for, or deprecated from the 15.0 software releases.

**Important:** All functionality from Limited Availability Release StarOS Version 14.1 has been included in General Availability Release StarOS Version 15.0. The *Cisco ASR 5x00 Release Change Reference, Version 14.1*, details new feature descriptions and configuration, performance, and security changes for the 14.1 release.

**Important:** Enhancements to SNMP MIBs in release 15.0 are located in the *SNMP MIB Changes* chapter. Enhancements to Web Element Manager (WEM) in release 15.0 are located in the *Web Element Manager Changes* chapter.
AAA Enhancements for February 27, 2015

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.

---

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

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

**Feature Changes**

**Parsing of Event Trigger for USAGE_REPORT**

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

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

---

**CSCur89572, CSCus36547, CSCur13994 - Diameter support for ‘EPS-Location-Information’ AVP**

**Applicable Products:** MME

**Feature Changes**

**AVP Support for Spec Compliancy Requirements**

This feature enables MME to send UE current location information or last known location information through “EPS-Location-Information” AVP in the Insert-Subscriber-Data-Answer (IDA) message. This AVP is signaled from MME to HSS through the S6a interface in order to comply with 3GPP TS 29.272 v11.9.0 specification.
AAA Enhancements for October 31, 2014

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

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

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

**Applicable Products:** P-GW

**Feature Changes**

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

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

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

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

**Feature Changes**

**Parsing of QoS-Information AVP in dpca-custom19 Dictionary**

- **Previous Behavior:** QoS-Information AVP will always be sent in CCR message for custom Gx dictionary “dpca-custom19”.
- **New Behavior:** QoS-Information AVP will not be sent always. This behavioral change is made to avoid the risk at the customer’s PCRF with more signaling than it can handle.

### CSCuQ06614 - Radius AVP SN-Rad-APN-Name to be added in custom67

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

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

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

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

If the RADIUS returned APN Name is invalid, the call will be dropped. Also, SN1-VIRTUAL-APN-NAME is not sent in accounting message even if SN1-RAD-APN-Name is sent in access accept.
AAA Enhancements for June 6, 2014

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

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

**Command Changes** - changes to any of the CLI command syntax. For details, refer to the *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.

---

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

**Applicable Products:** ePDG

**Feature Changes**

**Change in Session Disconnect Reason Value**

**Previous Behavior:** For authentication rejection from AAA server, the session disconnect reason was set for invalid-aaa-attribute.

**New Behavior:** The session disconnect reason is set to auth-failure when the session is rejected by AAA server due to authentication failure.

---

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

**Applicable Products:** PDSN

**Feature Changes**

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

To support accepting CCR messages on Gx interface, customer should configure the Diameter dictionary “dpca-custom28” in IMS Authorization Service configuration mode.

---

**CSCum36361 - No CCR-T when diameter failover from primary to secondary diameter host**

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

Support for Dynamic Route Creation

**Previous Behavior:** Dynamic route was not added for server-initiated messages.

**New Behavior:** Dynamic route is now created when server-initiated messages are received in the Diameter failure handling scenario.

**CSCun52379 - Redirection when RC4012 or RC4010 at MS CC level with FUI redirect**

**Applicable Products:** GGSN

Feature Changes

Support for FUI Redirection for 4010/4012 Result Codes

In this release, FUI redirection will happen even when 4010/4012 result-codes are received in CCA-I or CCA-U at MSCC level.
AAA Enhancements for April 30, 2014

This section identifies all of the AAA (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 *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.

CSCul85477 - PGW not setting the T flag & changing the E2EID on Gx retransmission

Applicable Products: eHRPD, GGSN, P-GW

**Feature Changes**

**Configuration Support for Setting T bit and Sending Same E2E on Retransmissions**

When one of the PCRF servers is down, and if failure-handling is set to “retry-and-terminate” the CCR messages from gateway is retried to the secondary PCRF. As per RFC 3588, the T bit must be set for retried messages so that the PCRF can identify duplicate messages. The End-to-End Identifier (E2E ID) has to remain the same. This feature is applicable to Gy and Rf messages as well.

**Previous Behavior:** When Diameter message is retried, the T bit was not set in the message as well as a different End-to-End Identifier (E2E ID) is sent in the retried message.

**New Behavior:** New CLI configuration options are introduced to set T-bit in a retried message along with having same End-to-End ID. Similar CLI command for setting T-bit is present under Credit Control Group configuration mode, which when configured will take effect for Gy messages else endpoint configuration will be used.

**Command Changes**

```bash
app-level-retransmission
```

This is a new command added in the Diameter endpoint configuration to set T-bit in a retried message along with having same End-to-End Identifier for application-level retries.

```bash
configure
  context context_name
    diameter endpoint endpoint_name
      [ default | no ] app-level-retransmission { retain-e2e | set-retransmission-bit }
```
end

Notes:

- Similar CLI command for setting T-bit is present under Credit Control Group configuration mode, which when configured will take effect for Gy messages else endpoint configuration will be used.
AAA Enhancements for March 31, 2014

This section identifies all of the AAA (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 *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.

---

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

*Applicable Products:* PDSN

**Feature Changes**

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

To support accepting CCR messages on Gx interface, customer should configure the Diameter dictionary “dpca-custom28” in IMS Authorization Service configuration mode.

---

**CSCuh43130 - Server unreachable condition is hit without behavior trigger configured**

*Applicable Products:* GGSN, P-GW

**Feature Changes**

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

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

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

**New Behavior:** If the retry happens due to server unreachable or normal failure handling or failure handling template, the servers unreachable state is hit only when there is a exact matching behavior trigger applicable for the retried
message. Server unreachable is not hit for the above mentioned result codes without the corresponding behavior trigger for dictionaries other than deca-custom13.
AAA Enhancements for January 31, 2014

This section identifies all of the AAA (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 *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.

CSCuh51285 - Always send Supported-Features AVP in CCR-U

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

**Feature Changes**

**Encoding of Supported-Features AVP in CCR-U**

**Previous Behavior:** The Supported-Features AVP was not encoded in CCR-U messages, but it was supported only in CCR-I message.

If Rel. 8 dictionary or any dictionary beyond Rel. 8 is used and PCRF does not provide Supported-Features AVP in CCA-I, then the call gets dropped.

The Supported-Features AVP is used during session establishment to inform the PCRF about the required and optional features that the PCEF supports.

**New Behavior:** If PCEF configures Diameter dictionary as release 8, 9 or 10, then PCRF sends Supported-Features AVP so that PCEF will know what feature PCRF supports. If PCEF receives supported features lesser than or greater than requested features then supported feature will be mapped to the lower one.

Whenever the custom dictionary "dpca-custom24" is configured, the Supported-Features AVP including Vendor-Id AVP will be sent in all CCR-U messages.

CSCuh96548 - Send 3GPP-Charging-Characteristics in CCR-I over Gx

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

**Feature Changes**

**Inclusion of 3GPP-Charging-Characteristics AVP in CCR-I**

**Previous Behavior:** Currently, ASR5K sends 3GPP-Charging-Characteristics AVP only for Gy interface but not for Gx interface. That is, this AVP is not included in CCR-I messages sent over the Gx interface.
For release 8 standard dictionary, QoS information was required in CCA-I message to establish the session. Hence, if this information is not available, then the call gets dropped.

**New Behavior:** This feature introduces the support for including 3GPP-Charging-Characteristics AVP in the Gx interface as well. Whenever the 3GPP Rel.8 based Diameter dictionary "dpca-custom24" is configured in PCEF and PCRF, the "3GPP-Charging-Characteristics" AVP is sent in CCR-I messages. The call is not rejected if QoS information is not received in CCA-I messages.

Though sending of this AVP over Gx is not defined in the 3GPP standards, this AVP is required for a Diameter Proxy between GGSN and PCRF/OCS Servers to perform server selection depending on subscriber’s plan, which is based on one of the Charging Characteristics value (15) provisioned in HLR.

**CSCul89329 - dpca-custom24:call dropped if Supported-feature AVP absent in CCR-I**

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

**Feature Changes**

**Modifications to dpca-custom24 Dictionary**

**Previous Behavior:** If 3GPP Rel. 8 dictionary or any dictionary beyond Rel. 8 is configured, then it is mandatory to receive Supported-Features AVP from PCRF. Otherwise, the calls gets dropped.

**New Behavior:** In this release, the Rel.8 based dictionary "dpca-custom24" is modified to accept the session without the presence of Supported-Features AVP in CCA-I message. The value that is configured in PCEF through the command "diameter update-dictionary-avps" in Policy Control Configuration mode will be considered for the session.
AAA Changes in Release 15.0
AAA Enhancements for November 30, 2013

This section identifies all of the AAA (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 *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.

### CSCub91633 - Header Enrichment: Customer-ID from RADIUS

**Applicable Products:** P-GW

**Feature Changes**

**Encoding of SN-Customer-ID AVP in RADIUS Auth Accept Message**

A new AVP “SN-Customer-ID” has been included in RADIUS Auth Accept message. This attribute carries the internal customer ID that will be used for HTTP header enrichment.

### CSCuc80426, CSCud28221 - PCC-Level report is not triggered when same mon-key for sess/pcc is used

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

**Feature Changes**

**Retrying Mechanism Added for Usage Monitoring Information**

**Previous Behavior:** When threshold breach happens for multiple monitoring keys at the same time, only one of the monitoring key’s usage is reported and the rest of the monitoring keys’ usage is reported in CCR-T (threshold set to infinity).

On Tx expiry/TCP link error, unreported usage is stored at ECS and reported only on session termination.

**New Behavior:** When threshold breach happens for multiple monitoring keys at the same time, only one of the monitoring key’s usage is reported first. Upon receiving successful response from PCRF, the rest of the monitoring keys’ usage is reported to PCRF.

On Tx expiry/TCP link error, unreported usage is stored at ECS. Any future successful interaction with PCRF for the session will send unreported UMI to PCRF.

With the introduction of retrying mechanism, there will not be any loss in the usage information.

For details, see the *Gx Interface Support* Appendix in the Administration Guide for the Product that uses Gx interface.
CSCue65856 - Local-policy to support TFT based on UE address request type

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

Feature Changes

Rule Matching based on PDN Type

Previous Behavior: Local policy did not have a control on the type of rules that it installs for a subscriber. It used to install v4 filter for v6 PDN and the UE which was holding a v6 address, rejected v4 filters.

New Behavior: New CLI option is added to local policy, which provides the intelligence to install the actiondefs/filters based on the UE PDN type/IP address allocated to the subscriber.

The rules in actiondef should be configured such that it matches with the PDN type in ruledef.

Command Changes

condition

Local Policy Ruledef CLI command is modified to accommodate the PDN Type as one of the rule matching parameters. That is, to intelligently install filters from Local Policy, a new variable “pdn-type” is added at local policy to push the filters based on the UE PDN Type.

configure

  local-policy-service service_name

  ruledef ruledef_name

    condition priority priority { pdn-type { eq | ge | gt | le | lt | match | ne | nomatch } regex | string_value | int_value | set }

    no condition priority priority

  end

Performance Changes

show local-policy statistics all

The following field has been added to perform a rule matching based on the PDN Type.

- PDN Type

CSCuh84653 - Gx: RAT-Type: EHRPD (2003) support required for eHRPD call

Applicable Products: P-GW
Feature Changes

Support for RAT-Type on eHRPD

**Previous Behavior:** The RAT-Type AVP was populated as HRPD (2001) in CCR messages for an eHRPD call.

**New Behavior:** For an eHRPD call, for release 8 dictionary, the behavior is the same, i.e., the RAT-Type will be sent as HRPD (2001).

For an eHPRD call, for release 9 and beyond, the RAT-Type will be sent as EHRPD (2003) in Gx messages.

CSCui30541 - Subscription-ID AVP in CCR-I does not support MSISDN for RAT-type WLAN

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

Feature Changes

CLI based Encoding of Subscription-ID AVP

**Previous Behavior:** Subscription-ID AVP was encoded based on service-type and Diameter dictionary.

**New Behavior:** When IMS Authorization service encodes the Subscription-ID AVP, IMSA will first check whether or not the CLI command `subscription-id service-type` is configured. If the CLI is configured for the current service, then IMSA will encode the Subscription-ID AVP based on the configured subscription-ID type. This CLI takes more precedence than the default behavior.

If the CLI configuration does not encode any Subscription-ID AVP, then IMSA will encode this AVP based on the default behavior. For example, in GGSN/IPSG service, NAI support is not available. If this CLI command is configured for GGSN/IPSG service with NAI type, then based on CLI IMSA cannot encode any subscription-ID AVP. By this time default behavior (old behavior based on service-type and dictionary) will add the subscription-ID.

Command Changes

```
subscription-id service-type
```

This new CLI command has been added to support enabling required subscription-id types for various services. In this release, the Subscription-ID AVP will be encoded based on the configured subscription-ID type.

```
configure

context <context_name>

ims-auth-service <ims-auth-service_name>

  policy-control

    subscription-id service-type { closed_rp | ggsn | ha | ipsg | l2tplns | mipv6ha | pdsn | pgw } { e164 | imsi | nai }

    { default | no } subscription-id service-type { closed_rp | ggsn | ha | ipsg | l2tplns | mipv6ha | pdsn | pgw } { e164 | imsi | nai }
```
CSCuj16170 - IPSG does not update Timezone over Gx for RAT Type WLAN

Applicable Products: IPSG

Feature Changes

3GPP-MS-TimeZone AVP Support for WLAN RAT-Type

Previous Behavior: Whenever RADIUS Interim-Update carries new Timezone value and 3GPP-RAT-Type value 03 (WLAN), IPSG does not include 3GPP-MS-TimeZone AVP in the Diameter CCR-U messages sent over Gx even though it includes respective event triggers into them. The same is observed if RAT type value 03 (WLAN) was already applied.

New Behavior: 3GPP-MS-TimeZone AVP is now encoded in CCR-U for any change in timezone when RAT Type is set to WLAN.

CSCuj20238 - [Gn-Gp] - 3GPP-User-Location-Info missing in 2nd INTERIM SDC-3g-4g-3g HO

Applicable Products: GGSN, P-GW

Feature Changes

3GPP-User-Location-Info AVP in Interim Record for RAI_CHANGE

Previous Behavior: In the scenario where the first INTERIM_RECORD generated for RAT_CHANGE from 3G to 4G contains RAI_CHANGE as one of the Change Conditions, then the 3GPP-User-Location-Info AVP was not present in the SDC of the next INTERIM_RECORD generated for RAT_CHANGE from 4G to 3G.

New Behavior: Now, the support has been extended for RAI_CHANGE as well. That means, the 3GPP-User-Location-Info AVP will be included in the second INTERIM_RECORD for both LOCATION_CHANGE and RAI_CHANGE event triggers.

CSCuj54761 - PGW: Gx rel 10 packet filter - Wrong TFT in CREATE_BEARER_REQUEST

Applicable Products: P-GW

Feature Changes

Flow-Direction AVP for Packet Filter Classifier

Previous Behavior: When Flow-Direction AVP is configured in Flow-Information AVP, ECS is not receiving correct direction value from IMSA. There is also a mismatch of ENUM values for Flow-Direction AVP. Because of this, GTP
is also sending the wrong direction. Hence, the value of Flow-Direction AVP received in Flow-Information AVP was ignored.

**New Behavior:** ENUMs of direction of packet filter from IMSA are modified to be in sync with 3GPP Rel.10 Gx standards. In this release Flow-Direction, if present, will be considered for determining the final direction of the packet filter. Flow-Direction is parsed at IMSA. ECS needs to process it and apply to dynamic rules.

**CSCuj97199 - CCR-T is not triggered when 5003 error is received**

**Applicable Products:** IPSG

**Feature Changes**

**Triggering of CCR-T on Permanent Failure**

**Previous Behavior:** CCR-T was sent when permanent failure result code is received in CCA-U and the Failure Handling (FH) template is configured with CCFH action as Terminate.

**New Behavior:** CCR-T is now triggered when permanent failure result code is received in the CCA-U and the FH template is configured with CCFH action as Terminate.

**CSCul12311 - authorize-with-hss ima report-ipv6-addr" is not working with custom17**

**Applicable Products:** P-GW

**Feature Changes**

**Inclusion of Framed-IPv6-Prefix and Framed-Interface-Id**

With this release, the Framed-IPv6-Prefix and Framed-Interface-Id attributes are included in the AAR message for the s6b dictionary "aaa-custom17".
AAA Enhancements for September 30, 2013

This section provides information on AAA accounting management changes available in release 15.0.

Diameter Accounting Management Changes as of September 30, 2013

This section provides information on Diameter accounting management changes available in release 15.0.

Diameter Feature Changes

This section identifies Diameter feature changes available in release 15.0.

**Important:** For more information regarding features in this section, refer to the *AAA Interface Administration and Reference* for this release.

New Diameter Features

This section identifies new Diameter features available in release 15.0.

**CLI-based Reauthorization of Blacklisted Content by RAR**

**Applicable Product(s):** GGSN, HA, IPSG, PDSN, P-GW, SAEGW

The current Gy implementation does not allow reauthorization of Blacklisted content (blacklisted with Result-Code like 4012, 4010, etc) when Gy receives an RAR (either a RG based RAR or generic RAR).

This feature determines if the RAR received from OCS is generic or to any specific rating-group.

If it is a generic RAR:

- If this CLI command “`diameter reauth-blacklisted-content`” is configured, then reauthorize all the Rating-Groups (RGs) which are blacklisted. CCR-U forced-reauthorization will be triggered all the RGs.
- If this CLI command “`diameter reauth-blacklisted-content content-based-rar`” is configured, then RG which are blacklisted will not be reauthorized. CCR-U forced-reauthorization will be triggered only for active RGs alone.

If Rating-Group information is received in RAR:

- If either “`diameter reauth-blacklisted-content`” or “`diameter reauth-blacklisted-content content-based-rar`” is configured, then RG gets re-authorized even it is blacklisted. CCR-U forced-reauthorization will be triggered for the received RG.

If this CLI command is not configured then the default behavior which is not to reauthorize blacklisted RG persists.

From Release 15.0, Gy RAR can be configured to allow Reauthorization of Blacklisted content (blacklisted with Result-Code like 4012, 4010, etc).

For more information, refer to the [diameter reauth-blacklisted-content](#) section in this chapter.

**Dynamic APN Configuration via S6b**

**Applicable Product(s):** eWAG, GGSN, IPSG, PDSN, P-GW
This feature is developed to implement a single global APN for the Enterprise services with the ability to have separate virtual APNs per single Enterprise, group of Enterprises sharing the same service group or per department.

To implement this feature, a configurable option is introduced per interface Rf, Gx, Gy and per APN. That is, a service specific CLI “apn-name-to-be-included” is configured for interfaces Rf, Gx, Gy separately. It can take values 'gn' or 'virtual'. Based on the value configured for this command, the Called-Station-Id AVP is populated.

The name of the virtual APN and the IP pool are signaled during the UE attach to the Enterprise PDN from the 3GPP AAA server over S6b interface with a new vendor-specific AVP “Virtual-APN-Name”. The RADIUS Start, Gy CCR to OFCS and Rf ACR to OCS messages contain the Virtual APN name instead of the Enterprise APN.

This feature provides customers the desired granularity per enterprise and per department. This also allows bundling of number of small enterprises under the umbrella of single APN and logically separating them by virtual APN.

For more information, refer to the apn-name-to-be-included section in this chapter.

Generic Rate Limiting Feature

**Applicable Product(s):** GGSN, MME, P-GW

**Important:** Rate Limiting Function (RLF) 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.

This feature implements a generic framework that can be used by multiple interfaces and products for rate-limiting/throttling outgoing messages like Diameter messages on Gx, Gy interface towards PCRF.

When applications send messages to peers at a high rate, (e.g. when a large number of sessions goes down at the same time, accounting stop messages for all the sessions are generated at the same time) the peer may not be able to handle the messages at such high rates. To overcome this situation, the Rate Limiting Function (RLF) framework is developed so that the application sends messages at an optimal rate such that peer is capable of receiving all the messages and does not enter an overload condition.

When RLF feature is enabled, all the messages from the application are pushed to the RLF module for throttling and rate control, and depending on the message-rate configured the RLF module sends the messages to the peer. Once the rate or a threshold value is reached, the RLF module notifies the application to slow down or stop sending messages. RLF module also notifies the application when it is capable of accepting more messages to be sent to the peer. RLF module typically uses a Token Bucket Algorithm to achieve rate limiting.

For more information, refer to the rlf-template section in this chapter.

Gx: Configurable Option to Send CCR-T on Call Termination

**Applicable Product(s):** GGSN, P-GW

The “msg-type” CLI with the retry-and-terminate and terminate failure-handling actions set in failure handling template has been extended to control sending of CCR-T when the call terminates.

This feature helps the customers to know when the subscriber connection is down and accordingly clear the hanging sessions.

IMSA Support for SRVCC PS-to-CS Handover Indication

**Applicable Product(s):** P-GW

Single Radio Voice Call Continuity (SRVCC) is an LTE functionality that allows a VoIP/IMS call in the LTE packet domain to be moved to a legacy voice domain (GSM/UMTS or CDMA 1x).
Present release of P-GW supports SRVCC PS-CS handover. Post handover completion, all dedicated bearers get deactivated and the associated rules get deleted by ECS upon release bearer instruction from Session Manager. However, ECS is unaware of this hand-over situation and also it does not generate any charging rule failure indication to the Session Manager in response to release bearer indication. Due to this, PCRF is unaware of why a rule is deleted by PCEF.

In this release, a new rule failure code PS_TO_CS_HANDOVER(13) is supported. When an IP-CAN bearer is deleted due to SRVCC, the PCEF is notifying the PCRF the exact reason for PCC rule deactivation.

When the IP-CAN bearer is terminated due to PS to CS handover, then P-GW sends a Charging Rule Report with rule failure code set to PS_TO_CS_HANDOVER. The PCEF reports the related PCC rules for this IP-CAN bearer by including the Rule-Failure-Code AVP set to the value PS_TO_CS_HANDOVER.

**LMA-coupled Web Authentication using Gx**

**Applicable Product(s):** P-GW

WebAuth is a standard for authentication to Wireless LAN access. In this method, the subscriber is always redirected to a Web portal on associating to the WiFi network and is expected to enter his/her credentials into the Web portal. The subscriber creates a PMIPv6 binding between the Mobile Access Gateway (MAG) and Local Mobility Anchor (LMA) prior to being redirected to the Web portal. Upon successful validation of the credentials, the subscriber is allowed to access any website of his/her choice. The subscriber does not have to provide his/her credentials even after a handoff to another Access Point within the same WiFi access area.

For Web authentication, the Subscription-Id and User-Equipment-Info AVPs are populated in the Mobile Link Layer Identifier Option (LLID) AVP in the Proxy Binding Update (PBU) message from the MAG to the LMA using the S2a PMIPv6 interface.

While authorizing the subscriber with PCRF, P-GW sends the User Equipment Info with the MAC address to PCRF instead of subscription ID.

> **Important:** The feature changes are applicable to the r8-gx-standard dictionary.

**NAPTR-based Dynamic HSS Discovery**

**Applicable Product(s):** SGSN

In releases prior to R15.0, the SGSN could contact a HSS only through static configuration of the HSS peer end point through the HSS service. From Release R15.0 onwards, dynamic peer discovery is supported. The HSS address will be resolved using NAPTR based DNS request-response method. The following commands have to be enabled for dynamic peer discovery:

- In the Context Configuration Mode, the command `diameter endpoint < endpoint_name >` has to be enabled.
- In the Diameter Endpoint Configuration Mode, the command `dynamic-peer-discovery [ protocol { sctp | tcp } ]` has to be enabled.
- In the Diameter Endpoint Configuration Mode, the command `dynamic-peer-realm < realm_name >` has to be enabled.
- In the Diameter Endpoint Configuration Mode, the command `dynamic-peer-failure-retry-count < no_of_retries >` has to be enabled.

The “realm name” is used for dynamic peer discovery. The “dynamic-peer-failure-retry-count” is used to configure the number of re-tries in peer discovery.
New Diameter AVPs on S6b

**Applicable Product(s):** GGSN, P-GW

To enable virtual APN signaling on S6b, a new vendor-specific AVP “Virtual-APN-Name” has been added to the S6b dictionary. This optional AVP is included in the AAA message sent over the S6b interface.

New Gy Dictionary to Support LNS/PDSN/HA

**Applicable Product(s):** HA, PDSN

A new dictionary is created based out of Gy standards for PDSN services and associated with dcce-custom29 in credit-control group. If this dictionary is configured, then Subscription-Id-Type AVP will be encoded always with the value "END_USER_IMSI" in the CCR-I message from PDSN.

New Rule Failure Codes

**Applicable Product(s):** GGSN, HA, HSGW, IPSG, PDSN, P-GW, S-GW

The following two new rule failure codes have been added to Rule-Failure-Code AVP:

- **INCORRECT_FLOW_INFORMATION**
  An IP-CAN session is identified by an IPv4 address and/or an IPv6 prefix. When both addresses are assigned to an IP-CAN session, the PCRF provides PCC rules with flows that include IPv4 addresses or IPv6 prefixes/addresses in the Flow-Description AVP. When only one IP version is supported, the PCC rules only include IP addresses/prefixes corresponding to the version supported by the IP-CAN session. If PCRF provides incorrect versions of IP addresses, the PCEF reports a specific error.

- **NO_BEARER_BOUND**
  If the PCC rule(s) that include the Rule-Activation-Time AVP are bound to a bearer that will require traffic mapping information to be sent to the UE, the PCEF reports the failure to the PCRF by including the Charging-Rule-Report AVP with the Rule-Failure-Code set the value “NO_BEARER_BOUND (xx)” for the affected PCC rule(s) identified by the Charging-Rule-Name AVP in either a CCR or an RAA command.

These new rule failure codes are added in the Gx dictionaries “dpca-custom15” and “r8-gx-standard”.

In addition to this, the name of old rule failure code 9 is changed to MISSING_FLOW_INFORMATION. For 3GPP Rel.10, rule failure code 9 maps to GW/PCEF_MALFUNCTION.

New Schemas and Bulkstats Support for RLF

**Applicable Product(s):** GGSN, MME, P-GW

New schemas “rlf” and “rlf-detailed” are added to support RLF related bulkstatistic collection. Some bulkstatistic variables are added to each of these new schemas. For the complete list of variables, see the New in the RLF Schema and New in the RLF-Detailed Schema sections in this chapter.

NI-LR Messages on SLg

**Applicable Product(s):** MME

This feature implementation involves sending a new server initiated message “Location-Report-Request” on the SLg interface to inform the LCS client about the UE information (on SLg interface), when an emergency call is received.

RAN Bandwidth Optimization

**Applicable Product(s):** P-GW
When the rule is installed and active, P-GW uses the GBR/MBR assigned in the rule for calculating the GBR / MBR values towards the bearers created. When more than one rule is installed, P-GW adds the GBR / MBR values from all the active and installed rules even if the flow of a certain rule is marked as disabled. This current behavior is in accordance with 3GPP TS standard specification 29.212, and this might result in RAN bandwidth wastage. To avoid this wastage, some optimization is done while calculating MBR and GBR for GBR bearer.

This optimization feature provides the ability to configure a list of APNs, for which the optimized calculation of MBR, GBR can be enabled. By default, this optimized calculation should be enabled only for the IMS APN.

This feature further helps optimize the logic of aggregating MBR and GBR values, based on “Flow-Status” AVP value received in the rule definition through RAR. This feature is controlled through the CLI command “ran bandwidth optimize”.

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

Result-Code based Bulk Statistics Support for Gx Messages

Applicable Product(s): GGSN, HA, HSGW, IPSG, PDSN, P-GW, S-GW

Bulkstats support has been added to IMS Authorization to display statistics based on result code. This statistics is pegged every time PCRF responds with an error result code.

New statistics counter variables are added to the output of the CLI command “show ims-authorization policy-control statistics”.

Selective TFT Suppression for Default Bearer

Applicable Product(s): P-GW

A new configurable option is provided to suppress selected TFT updates to the UE. This is provided by specific charging-action level option to identify if the appropriate TFT defined in the charging action needs to be sent to the UE or not. This CLI is supported for both default and dedicated bearer.

One more new CLI to suppress TFTs on default bearer has been added, so the operator has the flexibility to configure this per Rulebase and also configure to suppress TFT updates only. This CLI allows sending other QoS updates to the UE and is only controlling TFT related updates. This CLI is supported only for default bearer.

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

Support for APN AMBR and EPS Bearer QoS Modification Failure Event Triggers

Applicable Product(s): GGSN, HA, HSGW, IPSG, PDSN, P-GW, S-GW

This feature provides support for the following new event triggers as per the 3GPP standard specification TS 29.212.

- APN_AMBR_MODIFICATION_FAILURE (29) – The PCEF uses this value to indicate to the PCRF that APN-AMBR modifications have failed. The PCEF uses this value in a new CCR command that indicates the failure of either a PUSH initiated modification or a PULL initiated modification. This event trigger needs no subscription.

- DEFAULT_EPS_BEARER_QOS_MODIFICATION_FAILURE (34) – The PCEF uses this value to indicate to the PCRF that Default EPS Bearer QoS modifications have failed. The PCEF uses this value in a new CCR command that indicates the failure of either a PUSH initiated modification or a PULL initiated modification. This event trigger needs no subscription.

This feature is triggered when QoS installation failure occurs at MME. The feature changes impact the Gx dictionaries that are configured as r8-gx-standard, dpca-custom15 and dpca-custom19.

Support for Charging Correlation Exchange over Gx
Applicable Product(s): GGSN, HA, HSGW, IPSG, PDSN, P-GW, S-GW

PCRF should know the charging identifier assigned to the bearers to correlate the charging information. PCRF requests the PCEF to provide the Access-Network-Charging-Identifier-Gx AVP associated to dynamic rules. To support this, the PCRF provides the Event-Trigger AVP with a new value CHARGING_CORRELATION_EXCHANGE (28) and a new Charging-Correlation-Indicator AVP indicating CHARGING_IDENTIFIER_REQUIRED within the Charging-Rule-Install AVP.

This feature implementation impacts the Gx dictionary “dpca-custom15”. This feature is only supported for dynamic rules as per standards.

**Previous Behavior:** The AVP “Access-Network-Charging-Identifier-Gx” was always sent in the CCR-U message. This AVP was also sent in RAA message by the chassis.

**New Behavior:** This AVP is sent in CCR-U only when event trigger 28 is enabled and the new AVP “Charging-Correlation-Indicator” is sent by PCRF to the chassis.

This AVP is not sent in RAA but a new CCR-U is triggered if the chassis receives Charging-Correlation-Indicator AVP in RAR message and trigger is enabled.

PCRF installs the trigger and requests for the charging correlation while installing/modifying a dynamic rule in RAR/CCA. PCRF installs the trigger and requests for charging correlation alone without modifying the rule in RAR/CCA message.

If the update of the rule changes the QCI/ARP of the rule and this leads to binding of the rule to a different bearer, the chassis sends out CCR-U to PCRF indicating the new charging ID in Access-Network-Charging-Identifier-Gx AVP.

---

**Important:** This behavior change is applicable only for dpca-custom15 and r8-gx-standard dictionaries and is valid for bearer type GTP and PMIP only.

In the case of RAR, when Charging-Correlation-Indicator AVP is present and event trigger 28 is present in RAR and Supported Features is Rel. 10 at both PCRF and chassis, CCR-U will be sent for all bearers.

**Support for Peer Selection at Diabase**

Applicable Product(s): GGSN, P-GW

In the earlier Gx implementation, Diameter Policy Control Application has the limitation to mandatorily configure hosts as part of IMS Authorization service or associate a host template and select the hosts to be communicated for each subscriber session. Since the peer selection can happen at diabase and application need not select any hosts, this feature is developed to remove the restrictions imposed in the application and allow diabase to pick the peers in a round robin fashion. In addition, this feature will take care of peer selection at diabase even when the hosts picked by application are not active. This change in behavior is controlled through the CLI command “endpoint-peer-select” as the default behavior is to drop the call if the server discovery fails at application.

When the peers are selected from endpoint, the output of CLI command “show ims-authorization sessions full” does not display these fields “Primary PCRF Server” and “Secondary PCRF Server”.

For more information on the command, refer to the endpoint-peer-select section.

**Support for PS-Furnish-Charging-Information in Gy**

Applicable Product(s): GGSN, P-GW

Support is added to all DCCA Gy dictionaries for parsing the PS-Furnish-Charging-Information AVP received in CCA message. The Furnish Charging Information (FCI) feature is based on the 3GPP standard specification 32.251.

FCI when received in CCA will be parsed in the PGW-CDRs if both online and offline charging are enabled.
Also, note that the FCI will be included in the CDRs only when the “furnish-charging-information” attribute is configured in the GTPP Group configuration mode. By default, this attribute is disabled.

**Support for Sponsor Identity over Gx**

**Applicable Product(s):** GGSN, P-GW

With Sponsored Data Connectivity, the sponsor has a business relationship with the operator and the sponsor reimburses the operator for the user's data connectivity in order to allow the user access to an associated Application Service Provider's (ASP) services. Alternatively, the user pays for the connectivity with a transaction which is separate from the subscriber's charging. It is assumed the user already has a subscription with the operator.

Sponsored Data Connectivity feature is introduced in Rel. 10 of 3GPP TS 29.212 specification. If Sponsored Data Connectivity is supported, the sponsor identity for a PCC rule identifies the 3rd party organization (the sponsor) who is willing to pay for the operator's charge for connectivity required to deliver a service to the end user.

The purpose of this feature is to identify the data consumption for a certain set of flows differently and charge it to sponsor. To support this, a new reporting level “SPONSORED_CONNECTIVITY_LEVEL” is added for reporting at Sponsor Connection level and two new AVPs “Sponsor-Identity” and “Application-Service-Provider-Identity” have been introduced at the rule level.

A new CLI command “diameter encode-supported-features” has been added in Policy Control Configuration mode” to send supported features with Sponsor Identity. For more information on the command, see the Command Line Interface Reference.

Sponsored connectivity feature will be supported only when both P-GW and PCRF support 3GPP Rel. 10. P-GW advertises release as a part of supported features in CCR-I to PCRF. If P-GW supports Release 10 and also sponsored connectivity but PCRF does not support it (as a part of supported features in CCA-I), this feature is turned off.

This feature implementation impacts only the Gx dictionary “dpca-custom15”. Also note that this feature is supported only for the dynamic rules.

**Modified Diameter Features**

This section identifies Diameter features modified in release 15.0.

**Assume Positive Gy Enhancements**

**Applicable Product(s):** GGSN, HA, IPSG, PDSN, P-GW

The following are the enhancements implemented as part of the Assume Positive Gy feature:

- Configurable per error code treatment to enter assume positive mode
- Graceful session restart upon receipt of a 5002 error

**Configurable per Error Code Treatment**

This feature allows the customers to configure error result codes using the CLI command “servers-unreachable behavior-triggers” that will trigger entering assume positive mode on the fly for CCR-Initial and CCR-Update messages. CCR-Terminate message is currently not supported. Also to maintain backward compatibility i.e. in case of no servers unreachable behavior triggers configured for error result codes, the default hard coded values are applicable.

Any error result codes from the range 3xxx to 5xxx can be specified using the CLI commands. For more information on the command, refer to the servers-unreachable section in this chapter.

This feature has been implemented to provide more flexibility and granularity in the way assume positive mode is triggered for error result codes.

**Graceful Session Restart**
Graceful session restart upon receipt of a 5002 error code is supported for server retried CCR-U messages during assume positive state. Also, any unreported usage from the time, server retried CCR-U sent till CCA-I is received, will be reported immediately by triggering CCR-U with usages for the same.

Any pending updates are aborted once CCA-U with 5002 is received from the server. Also CCR-U is triggered immediately following session restart only if there are any unreported usages pending.

**Important:** When the server responds with 5002 error result code, it does not include any granted service units for the requested rating groups.

### Charging-ID AVP

**Applicable Product(s):** GGSN, P-GW

**Previous Behavior:** When EVENT_TRIGGER(28) is enabled PCEF reports default bearers’ Charging-Id value in Access-Network-Charging-Identifier-Gx AVP.

**New Behavior:** When EVENT_TRIGGER(28) is enabled and Charging-Correlation-Indicator AVP is present in dynamic rule-install, PCEF reports Charging-Id value of the bearer with which the dynamic rule is installed in Access-Network-Charging-Identifier-Gx AVP in CCR-U.

When this feature is enabled, PCEF reports additional Access-Network-Charging-Identifier-Gx AVP to PCRF whenever a rule is installed or modified.

### Configuration and Bulk Statistics Support for P-CSCF Address Allocation

**Applicable Product(s):** SAEGW

The existing CLI command to display the IMSA service configuration is enhanced to display P-CSCF server related counters by adding new options using which all server information or specific server information can be displayed.

New bulk statistic variables are added in the existing DPCA schema.

### Configuration Support for Usage Report Value in Event-Trigger AVP

**Applicable Product(s):** GGSN, PDSN, P-GW

The numerical value of the Event-Trigger AVP’s Usage Report has been changed a couple of times in the 3GPP TS 29.212 standard spec. As a result of that, the releases of TS 29.212 are not backward compatible. To address this, a new CLI command `diameter map usage-report { 26 | 29 | 33 }` has been introduced in Policy Control configuration mode to map the USAGE_REPORT to either 26/29/33 in order to be flexible enough to interoperate with various operators.

- TS 29.212 v9.5.0 - USAGE_REPORT (26)
- TS 29.212 v9.6.0 - USAGE_REPORT (29)
- TS 29.212 v9.7.0 - USAGE_REPORT (33)

For more information on the command, refer to the `diameter map usage-report` section.

### Display Changes for P-CSCF Server Address after Session Recovery

**Applicable Product(s):** SAEGW

**Previous Behavior:** The P-CSCF server addresses selected for a subscriber were displayed in the output of “show ims-authorization sessions full” command post session manager recovery.
**New Behavior:** P-CSCF server selection after session recovery is removed as P-CSCF addresses are required only during call establishment and not required at later stages of the session.

Hence, the P-CSCF server addresses selected for a subscriber are not part of the "show ims-authorization sessions full" output post session manager recovery.

**Encoding of 3GPP2-MEID AVP in CCR Messages**

**Applicable Product(s):** PDSN

**Previous Behavior:** MEID value was not encoded in CCR messages.

**New Behavior:** The 3GPP2-MEID AVP is added to dcca-custom16 and standard Gy dictionary. This AVP is part of Terminal-Information AVP. This optional AVP is sent in all CCR messages over Gy interface only if received on A11 interface.

This change is mainly implemented to charge and control the subscriber of data service by IMSI and MEID.

**Extended Support for Diameter Result-Codes 4202/4203**

**Applicable Product(s):** GGSN, P-GW

**Previous Behavior:** When the OCS sends CCA-U with MSCC result-code 4202 (USER_EXPIRED) and 4203 (USER_INVALID) and FUI = REDIRECT, these result codes were treated as failure result-codes.

**New Behavior:** For the Gy dictionary "dcca-custom30", when the OCS sends CCA-U with the result-code 4202/4203 and FUI = REDIRECT, these result-codes will be treated as success (redirection) result-codes (2001) and the subscriber will be redirected to the specified redirected URL.

**Failure Handling Configuration Change for Result Code 4010**

**Applicable Product(s):** GGSN

**Previous Behavior:** For postpaid subscribers, the default CCFH behavior with dcca-custom27 dictionary was set to "continue", when the transient failure result-code 4010 is received.

**New Behavior:** Fandling Handling template is used to overwrite the default behavior to “terminate” when the result-code 4010 is received.

**Gx Assume Positive Enhancement**

**Applicable Product(s):** GGSN, HA, HSGW, IPSG, PDSN, P-GW, S-GW

**Previous Behavior:** Once the IP CAN session falls back to local policy it remained with local policy until the termination timer expires or the subscriber disconnects.

Also, the RAR message received when the local-policy timer was running got rejected with the cause “Unknown Session ID”.

**New Behavior:** Now, P-GW/GGSN provides a fair chance for the subscriber to reconnect with PCRF in the event of CCR failure. To support this feature, configurable validity and peer backoff timers are introduced in the Local Policy Service and Diameter endpoint configuration commands.

Also, the RAR received when the local-policy timer is running will be rejected with the cause “DIAMETER_UNABLE_TO_DELIVER”.

**IMSI/MSISDN based PCRF Selection**

**Applicable Product(s):** GGSN, PDSN, P-GW
PCEF selects PCRF based on various algorithms. The current support is limited to round robin, ip-address-modulus and msisdn-modulus. In this release, selection of PCRF based on the IMSI range and MSISDN is supported.

The existing CLI command `host-select` in the Diameter Host Template Configuration mode is modified to enable the selection of peer based on the configured prefix/suffix/range values of IMSI or MSISDN of subscriber.

Once a row is selected the failure handling for the subscriber will be done based on the configuration. The primary and the secondary hosts configured can be picked up in an active standby mode or in round robin fashion.

**Previous Behavior:** In the Diameter host template configuration, overlapping range of IMSI or MSISDN values were not allowed and PCRF selection was based on exact match of IMSI/MSISDN.

**New Behavior:** The existing CLI command `host-select` in the Diameter Host Template Configuration mode is modified to allow overlapping range of IMSI or MSISDN values. PCRF selection is now performed based on the first match of prefix/suffix/range on row precedence priorities.

Length of IMSI or MSISDN range is same in any IMSI or MSISDN host template configuration list.

**Increased Field Size for HTTP User-Agent and URL in EDRs**

**Applicable Product(s):** GGSN, P-GW

**Previous Behavior:** The maximum field size allowed in the configuration of EDR rule-variable for http url and user-agent was 127. Any URL/User-Agent greater than 127 was truncated and then written to EDR. There were no limits checks placed by HTTP protocol for the length of these fields.

**New Behavior:** An optional filter “length” is supported for HTTP URL and User-Agent which when added will allow the user to configure length from 1 to 255.

**Logging Support for RLF**

**Applicable Product(s):** GGSN, MME, P-GW

New event IDs ranging from 204900 through 204999 are added to support logging related to Rate Limiting Function (RLF) feature.

**Rf Records Generation**

**Applicable Product(s):** P-GW

**Previous Behavior:** For tariff time trigger, if there is no data to report, then no SDC was included in the INTERIM.

**New Behavior:** For tariff time trigger, even if there is no data to report, an SDC will be included in the INTERIM record.

**Rule Matching based on PDN Type**

**Applicable Product(s):** P-GW

**Previous Behavior:** Local policy did not have a control on the type of rules that it installs for a subscriber. It used to install v4 filter for v6 PDN and the UE which was holding a v6 address, rejected v4 filters.

**New Behavior:** New CLI option is added to local policy, which provides the intelligence to install the actiondefs/filters based on the UE PDN type/IP address allocated to the subscriber.

The rules in actiondef should be configured such that it matches with the PDN type in ruledef.

**Support for AF-Charging-Identifier AVP on Gx**

**Applicable Product(s):** GGSN, P-GW, SAEGW
With this enhancement, it is now possible to populate the AF-Charging Identifier AVP and send it over the Gx interface.

**Support for AF-Correlation-Information AVP at MSCC Level**

**Applicable Product(s):** GGSN, P-GW, SAEGW

With this enhancement request, AF-Charging Identifier is received over the Gx interface. The charging ID received from PCRF is passed to OCS using the AF-Correlation-Information AVP. This AVP is now supported at Multiple-Services-Credit-Control (MSCC) level.

The Gy dictionary “dcca-custom7” is modified to include AF-Correlation-Information AVP as part of the grouped AVP “Multiple-Services-Credit-Control” in the CCR messages. The AF-Correlation-Information AVP is parsed in MSCC if the reporting level is SERVICE_IDENTIFIER_LEVEL and the respective parameters are received from PCRF.

*Important:* The AF-Correlation-Information AVP is included only if AF-Charging-Id is received from PCRF. Also, note that this enhancement applies to dynamic rule only.

**Support for PCRF Reconnection after Applying Continue Failure Handling Action**

**Applicable Product(s):** GGSN, P-GW

**Previous Behavior:** If failure-handling action “continue” is applied to a subscriber’s session, there was no further interaction with PCRF. The usage monitoring information was lost in the event of message delivery failure.

**New Behavior:** If this new CLI “continue retry-server-on-event” is configured in the Policy Control Configuration mode or with failure-handling template, CCR-U is sent to PCRF, even after failure action continue is taken for the subscriber.

When the message delivery fails, the usage monitoring information is restored at ECS (except last rule removal or if monitoring stopped) and reported in CCR-T or in the next CCR-U (if CLI “event-update send-usage-report” is configured).

**Support for Service-Start-Time AVP in dcca-custom28 Gy Dictionary**

**Applicable Product(s):** GGSN

The Diameter AVP "Service-Start-Time" is added as part of the CCR-I and CCR-U messages in the Gy dictionary "dcca-custom28". With the inclusion of this AVP in dcca-custom28, the operators can charge the subscriber's usage based on the start time of the services / rating group accordingly.

Note the subsequent CCR-U for that rating group retains the same Service Start Timestamp value. After Quota Holding Timer (QHT) expiry, the relevant service / rating group is considered closed once the CCA-U is received. The Service-Start-Timestamp AVP should be set according to the Event-Timestamp of the next CCR-U sent for that rating group.

**Support for Sponsor Identity**

**Applicable Product(s):** GGSN, P-GW

**Previous Behavior:** Only two reporting levels (0 – SERVICE_IDENTIFIER and 1 – RATING_GROUP) were initially supported.

**New Behavior:** One more reporting level (2 – SPONSORED_CONNECTIVITY_LEVEL) is now supported for reporting at Sponsor Connection level. This reporting level is currently applicable only for the dynamic-rules and if offline charging is enabled.

If the offline charging is enabled and the reporting level is 2 then both the AVPs “Sponsor-Identity” and “Application-Service-Provider-Identity” must be present for the rule installation/update procedure to succeed.
Support to Configure Release Compliance of Standard Dictionary

Applicable Product(s): SGSN

Previous Behavior: Diameter supports three dictionaries standard, standard-r9, and custom dictionary. The standard dictionary is 3GPP TS 29.272 Release 8 compliant and standard-r9 is 3GPP TS 29.272 Release 9 compliant. The operator could configure the required dictionary.

New Behavior: The standard-r9 and custom dictionaries are no longer supported. There will be only one standard dictionary. The standard dictionary which was 3GPP TS 29.272 Release 8 compliant in earlier releases, will now contain AVPs of Release 9 and Release 10 as well. A new CLI command `diameter update-dictionary-avps {3gpp-r10 | 3gpp-r9}` is introduced under the HSS Peer Service Configuration mode, to configure the release that has to be supported for the HSS Peer Service. This new command is applicable only for the standard dictionary and can be configured as either Release 9 or Release 10 compliant. The default standard dictionary has been retained as Release 8 compliant to ensure backward compatibility. The “no” form of the command can be used to disable the command.

Support for Vendor-Specific-Application-Id in S6d Interface

Applicable Product(s): SGSN

Previous Behavior: The Diameter implementation on SGSN does not send Vendor-Specific-Application-ID Grouped AVP in any Diameter application messages.

New Behavior: The SGSN now sends Vendor-Specific-Application-Id AVP in all S6d messages from the SGSN.

Important: Except in Reset-Answer, all other messages contain Vendor-Specific-Application-Id AVP.

Impact: The intermediate nodes have to decode the Vendor-Specific-Application-Id AVP.

UDR Tariff Time Feature Support

Applicable Product(s): PDSN

The PDSN/PCEF generates content base UDR record for each concurrent online subscriber in each of day cross and place them in a single UDR file. The charging records include content based service (by duration and by volume).

To support this feature, a new CLI command “udr trigger tariff-time” is introduced to configure “Tariff Time” trigger for UDR in ACS Rulebase configuration mode. This CLI command is configured to generate UDR at the specified tariff-time in rulebase.

Tariff time is stored at rulebase level. Therefore if the tariff time is updated while there are ongoing calls in the network, the old tariff time will be ignored and the new tariff time will be applied to the existing as well as upcoming calls.

At the end of the “Tariff Time” period, the UDR files are created and the next set of records are stored in a new UDR file.

Weight based P-CSCF Selection

Applicable Product(s): GGSN, P-GW, SAEGW

P-GW/GGSN discovers P-CSCF for a subscriber and assigns a P-CSCF address to the UE based on the P-CSCF address IE in PCO. Currently, PCEF supports allocating P-CSCF address from S6b/APN/IMSA configuration.

Within the IMS Authorization configuration, the P-CSCF address is selected based on round robin fashion. This feature allows the customer to perform P-CSCF selection based on weight factor.

In this release, a new CLI option to configure weight (in the scale of 1 to 10) is added to each row through the CLI command `p-cscf table row` under IMS Authorization Service configuration, and the rows are selected based on
weighted round-robin. That is, the row with higher weight parameter is selected more number of times than the row with less number of weights.

**Diameter Command Changes**

This section identifies Diameter command changes available in release 15.0.

---

**Important:** For more information regarding commands in this section, refer to the *Command Line Interface Reference* for this release.

**New Diameter Commands**

This section identifies new Diameter commands available in release 15.0.

**apn-name-to-be-included**

*Applicable Product(s):* GGSN, P-GW

This command configures the APN name to be included in the Rf messages. Based on the value configured for this command, the Called-Station-Id AVP is populated.

```
configure

context context_name

policy accounting policy_name

apn-name-to-be-included { gn | virtual }

default apn-name-to-be-included

end
```

If `apn-name-to-be-included` is set as default (gn), the Called-Station-Id AVP indicates the actual apn-name. If configured otherwise, then this AVP is populated with the virtual APN name.

**clear rlf-context-statistics**

*Applicable Product(s):* GGSN, MME, P-GW

This command clears the RLF statistics from the context.

```
clear rlf-context-statistics diamproxy [ endpoint endpoint_name [ peer-realm realm_name [ peer-host host_name ] ] ] [ | { grep grep_options | more } ]
```

---

**Important:** Rate Limiting Function (RLF) 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.

**delay-tolerance**

*Applicable Product(s):* GGSN, MME, P-GW
This command defines the maximum number of seconds the control plane signaling messages can be queued before it is processed. After exceeding this, the message is dropped.

```
configure

rlf-template rlf_template_name

delay-tolerance tolerance_value [ -noconfirm ]

default delay-tolerance

end
```

**Important:** Rate Limiting Function (RLF) 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.

diameter disable-final-reporting-in-ccru

This command controls sending of CCR-U with FINAL as reporting reason immediately on receiving a 4012 or 4010 result-code at MSCC level.

```
configure

require active-charging

active-charging service service_name

credit-control

diameter disable-final-reporting-in-ccru

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

end
```

If this CLI command is configured, on receiving the result-code 4010/4012 at MSCC-level, immediate CCR-U with FINAL as Reporting-Reason will not be sent. All USU corresponding to that rating group is reported in CCR-T message.

diameter enable-quota-retry

This command enables/disables Quota Retry Timer for blacklisted content.

```
configure

require active-charging

active-charging service service_name

credit-control

diameter enable-quota-retry end-user-service-denied

no diameter enable-quota-retry end-user-service-denied
```
end

If this CLI command is configured, after the quota-retry timeout, CCR-U including the RSU is sent for blacklisted content also. That is, quota will be requested for 4010 blacklisted content also.

**diameter encode-supported-features**

**Applicable Product(s):** GGSN, P-GW

This CLI command has been added in Policy Control Configuration mode to send Supported-Features AVP with Sponsor Identity.

```lua
configure
  context context_name
    ims-auth-service service_name
      policy-control
      diameter encode-supported-features sponsored-connectivity
    { default | no } diameter encode-supported-features
  end
```

The purpose of this feature is to identify the data consumption for a certain set of flows differently and charge it to sponsor. To support this, a new reporting level “SPONSORED_CONNECTIVITY_LEVEL” is added for reporting at Sponsor Connection level and two new AVPs “Sponsor-Identity” and “Application-Service-Provider-Identity” have been introduced at the rule level.

Sponsored Connectivity feature will be supported only when both P-GW and PCRF support 3GPP Rel. 10. P-GW advertises release as a part of supported features in CCR-I to PCRF. If P-GW supports Release 10 and also Sponsored Connectivity but PCRF does not support it (as a part of supported features in CCA-I), this feature is turned off.

This feature implementation impacts only the Gx dictionary “dpca-custom15”. Also note that this feature is supported only for the dynamic rules.

**diameter exclude-mscc-in-ccr-terminate**

**Applicable Product(s):** GGSN, IPSG

This command enables to exclude Multiple-Services-Credit-Control (MSCC) AVP in CCR-T message.

```lua
configure
  require active-charging
  active-charging service service_name
    credit-control
      diameter exclude-mscc-in-ccr-terminate
    { default | no } diameter exclude-mscc-in-ccr-terminate
  end
```
If this CLI command is configured, upon call termination, the system will send the usage reporting for all the rating groups in the CCR-U instead of sending it to CCR-T. This CLI command is also used to control sending of either single or multiple MSCC AVP in CCR messages.

**diameter map usage-report**

**Applicable Product(s):** GGSN, PDNS, P-GW

This CLI command enables selecting the value to which the USAGE_REPORT and APN_AMBR_MOD_FAILURE Event-Trigger should be mapped to.

```plaintext
configure

  context context_name

  ims-auth-service service_name

  policy-control

  diameter map usage-report { 26 | 29 | 33 }

  default diameter map usage-report

end
```

The Event-Trigger AVP’s USAGE_REPORT has been given different values in the 3GPP TS 29.212 standard spec. As a result of that, the releases of TS 29.212 are not backward compatible. To address this, this CLI command has been introduced in Policy Control configuration mode to map the USAGE_REPORT to either 26/29/33 in order to be flexible enough to interoperate with various operators.

- TS 29.212 v9.5.0 - USAGE_REPORT (26)
- TS 29.212 v9.6.0 - USAGE_REPORT (29)
- TS 29.212 v9.7.0 - USAGE_REPORT (33)

**diameter reauth-blacklisted-content**

**Applicable Product(s):** GGSN, HA, IPSG, PDNS, P-GW

This command allows reauthorization of blacklisted content (blacklisted with Result-Code like 4012, 4010, etc) when a Rating Group (RG) based Re-Authorization Request (RAR) or generic RAR is received.

This new CLI command is required to enhance the Blacklisted RG to get reauthorized on receiving RAR.

```plaintext
configure

  require active-charging

  active-charging service service_name

  credit-control

  diameter reauth-blacklisted-content [ content-based-rar ]

  no diameter reauth-blacklisted-content

end
```
**diameter update-dictionary-avps**

**Applicable Product(s):** MME, SGSN

A new CLI command `diameter update-dictionary-avps { 3gpp-r10 | 3gpp-r9 }` is introduced under the HSS Peer Service Configuration mode, to configure the release compliance of the Standard dictionary that is supported for the HSS Peer Service. This new command is applicable only for the Standard dictionary and can be configured as either Release 9 or Release 10 compliant. The default standard dictionary has been retained as Release 8 compliant to ensure backward compatibility. The “no” form of the command can be used to disable the command.

```plaintext
configure
  context context_name
    hss-peer-service service_name
      diameter update-dictionary-avps { 3gpp-r10 | 3gpp-r9 }
    end
end
```

**endpoint-peer-select**

**Applicable Product(s):** GGSN, HA, HSGW, IPSG, PDSN, P-GW, S-GW

This command is used to perform server selection at Diabase when the hosts could not be selected by application or when the hosts selected by the IMS Authorization application is inactive. For example, host table is not configured in IMSA service, host table is configured but not activated, none of the rows in prefix table match the subscriber, host template is not associated with IMSA service, host template could not select the hosts.

```plaintext
configure
  context context_name
    ims-auth-service service_name
      policy-control
        endpoint-peer-select [ on-host-select-failure | on-inactive-host ]
        { default | no } endpoint-peer-select
      end
end
```

This CLI command is added in policy control configuration mode to maintain backward compatibility with the old behavior of terminating the call when server selection fails at IMS Authorization application.

**msg-rate**

**Applicable Product(s):** GGSN, MME, P-GW

This command defines the number of messages that can be processed per second. In other words, this specifies the maximum allowed transactions per second (TPS) for an external interface. The RLF will ensure that the maximum configured TPS rate is not exceeded on the interface.
**Important:** Rate Limiting Function (RLF) 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.

```
configure
    rlf-template rlf_template_name
        msg-rate tps_value burst-size size [ -noconfirm ]
    end
```

**peer-backoff-timer**

**Applicable Product(s):** GGSN, HA, P-GW

This command is used to configure a peer backoff timer which will be started when the server (primary or secondary PCRF) is busy. That is, the backoff-timer is started when the result code 3004 – DIAMETER_TOO_BUSY is received from PCRF. No CCR-I messages will be sent to the server until this timer expires.

```
configure
    context context_name
        diameter endpoint endpoint_name
            peer-backoff-timer timeout [ send-app-level-term-req ]
            { default | no } peer-backoff-timer
    end
```

**ran bandwidth optimize**

This command is used to enable optimized calculation of [MBR, GBR] when a subscriber (voice) call is put on hold in case of VoLTE.

```
configure
    require active-charging
    active-charging service service_name
        rulebase rulebase_name
            [ default | no ] ran-bandwidth optimize
    end
```

During session setup, when a CCA-I is received, and if **ran bandwidth optimize** is configured for the associated rulebase, the system will aggregate [MBR, GBR] values of only the rules which have flow-status='ENABLED'. This information will subsequently be sent to UE.

By default, this CLI will be disabled. Any change in this configuration will not affect existing calls on the system. Optimized bandwidth calculation will be done only for the new calls established after enabling this CLI command.
rfl schema

Applicable Product(s): GGSN, MME, P-GW

This command is used to configure the aggregated information for Rate Limiting Function (RLF) context statistics schema.

Important: Rate Limiting Function (RLF) 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.

configure
  bulkstats mode

  rfl schema schema_name format schema_format

  no rfl schema schema_name

  end

rfl-detailed schema

Applicable Product(s): GGSN, MME, P-GW

This command is used to configure the detailed instance level information for RLF context statistics schema.

Important: Rate Limiting Function (RLF) 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.

configure
  bulkstats mode

  rfl-detailed schema schema_name format schema_format

  no rfl-detailed schema schema_name

  end

rlf-template

Applicable Product(s): GGSN, MME, P-GW

This command is used to enter the RLF Template Configuration mode. The users can define the rate limiting configurations within this template.

Important: Rate Limiting Function (RLF) 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.

configure
  rlf-template rlf_template_name
no rlf-template rlf_template_name
end

For more information on this feature, see the Global Configuration Mode Commands chapter of the Command Line Interface Reference.

rlf-template

Applicable Product(s): GGSN, MME, P-GW
This command configures the RLF template to be used for the Diameter endpoint for throttling and rate control.

Important: Rate Limiting Function (RLF) 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.

configure

context context_name
diameter endpoint endpoint_name
rlf-template rlf_template_name
no rlf-template rlf_template_name
end

show rlf-context-statistics

Applicable Product(s): GGSN, MME, P-GW
This command displays the statistics for all active RLF contexts.

show rlf-context-statistics diamproxy [ facility_num | [ endpoint endpoint_name [ peer-realm realm_name [ peer-host host_name ] ] ] | summary | verbose ] [ | { grep grep_options | more } ]

Important: Rate Limiting Function (RLF) 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.

show rlf-memcache-statistics

Applicable Product(s): GGSN, MME, P-GW
This command displays the memory used by RLF for processing the messages.

show rlf-memcache-statistics diamproxy facility_num [ | { grep grep_options | more } ]

Important: Rate Limiting Function (RLF) 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.
show rlf-template

Applicable Product(s): GGSN, MME, P-GW
This command displays the statistics for all active RLF templates.

```
show rlf-template { all | name template_name } [ | { grep grep_options | more } ]
```

Important: Rate Limiting Function (RLF) 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.

tft-notify-ue

Applicable Product(s): P-GW
This command allows you to suppress specific TFT updates from being sent to the UE. This way, the operators can
suppress any unwanted TFTs to the UE.

```
configure
    require active charging
    active-charging service service_name
        charging-action charging_action_name
            [ no ] tft-notify-ue
    end
```

tft-notify-ue-def-bearing

Applicable Product(s): P-GW
This command allows you to control whether TFT updates are sent to UE or not for default bearer for the specified
rulebase. This command allows sending other QoS updates to the UE and controls only the TFT related updates. This
CLI is supported only for default bearer.

```
configure
    require active charging
    active-charging service service_name
        rulebase rulebase_name
            [ default | no ] tft-notify-ue-def-bearing
    end
```

threshold

Applicable Product(s): GGSN, MME, P-GW
This command configures the threshold for rate-limiting the outgoing messages.
configure

rlf-template rlf_template_name

   threshold { lower lowerThreshold_value | upper upperThreshold_value } [ -noconfirm ]

   default threshold

end

**Important:** Rate Limiting Function (RLF) 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.

Modified Diameter Commands

This section identifies Diameter commands modified in release 15.0.

**action**

**Applicable Product(s):** GGSN, HA, P-GW

The local policy service configuration has been modified to retry to PCRF after a configured amount of time. This is achieved through the use of new option “retry-count” along with the action “start-timer”. New action “reconnect-to-server” is also added in the local-policy actiondef configuration to handle backoff scenario.

configure

   local-policy-service service_name

   actiondef actiondef_name

   action priority priority action_name arguments

   no action priority priority

end

**condition**

**Applicable Product(s):** P-GW

Local Policy Ruledef CLI command is modified to accommodate the PDN Type as one of the rule matching parameter. That is, to intelligently install filters from Local Policy, a new variable “pdn-type” is added at Local Policy to push the filters based on the UE PDN Type.

configure

   local-policy-service service_name

   ruledef ruledef_name

   condition priority priority { variable { eq | ge | gt | le | lt | match | ne | nomatch } regex | string_value | int_value | set }
AAA Changes in Release 15.0

AAA Enhancements for September 30, 2013

no condition priority priority
end

event-notif-service

Applicable Product(s): GGSN, HA, HSGW, IPSG, MME, PDSN, P-GW, S-GW

This command enables or disables the ORB Notification Service and allows the configuration of filters dictating which event notifications are sent. This command has been enhanced to support additional event IDs ranging from 204900 to 204999 for RLF related logging.

config

orbem

event-notif-service [ filter { event-id event_id [ to final_event_id ] } ]
no event-notif-service [ filter { event-id event_id [ to final_event_id ] } ]
end

event-update

Applicable Product(s): GGSN, HA, HSGW, IPSG, PDSN, P-GW, S-GW

This command has been enhanced to support a new event trigger “CHARGING_CORRELATION_EXCHANGE (28)” in the configuration. This is applicable only for dynamic rules.

configure

context context_name

ims-auth-service service_name

policy-control

event-update send-usage-report events { charging-correlation-exchange }
{ default | no } event-update
end

event-update

Applicable Product(s): GGSN, HA, HSGW, IPSG, PDSN, P-GW, S-GW

This command configures sending usage monitoring information in event updates either for all event triggers or for a specific event trigger. This command has been extended to support APN_AMBR_MODIFICATION_FAILURE and DEFAULT_EPS_BEARER_QOS_MODIFICATION_FAILURE event triggers in EPS 3.0.

If the modification of the QoS per APN fails, the PCEF will retain the existing QoS per APN without any modification and send to the PCRF a new CCR command with the Event Trigger set to APN_AMBR_MODIFICATION_FAILURE providing the retained value within the APN-Aggregate-Max-Bitrate-UL AVP and/or APN-Aggregate-Max-Bitrate-DL AVP included in QoS-Information AVP.
If the modification of the default EPS bearer QoS information fails, the PCEF will retain the existing default EPS bearer QoS without any modification and send the PCRF a new CCR command and include with Event Trigger set to DEFAULT_EPS_BEARER_QOS_MODIFICATION_FAILURE providing the retained values within the Allocation-Retention-Priority AVP and QoS-Class-Identifier AVP included in Default-EPS-Bearer-QoS AVP.

```
configure
  context context_name
    ims-auth-service service_name
      policy-control
      event-update send-usage-report events { apn-ambr-mod-failure | default-bearer-qos-mod-failure } +
      { default | no } event-update
    end
```

### failure-handling

**Applicable Product(s):** GGSN, HA, HSGW, IPSG, PDSN, P-GW, S-GW

A new optional keyword `retry-server-on-event` has been added to enable reconnecting with PCRF server on update and termination requests or re-authorization from server, for failure-handling CONTINUE sessions.

```
configure
  context context_name
    ims-auth-service service_name
      policy-control
      failure-handling cc-request-type update-request continue retry-server-on-event
      no failure-handling cc-request-type update-request
    end
```

### file

**Applicable Product(s):** GGSN, PDSN, P-GW, SGSN, S-GW

This command has been enhanced to accommodate the following new keywords:

- **unique-seq-num**: Ensures that the EDR records are created with independent sequence number. With this configurable option, the users can easily detect the loss of records. By default, all record types including (UDR, EDR, REDR and EVENT) share the same sequence number.

- **tariff-time minute**: Enables to rotate the file at a specific time/hour once per day.

| Important: | The options **time** and **tariff-time** are mutually exclusive and only any one of them can be configured. Other file rotation options can be used with either of them. |
configure

    context context_name

    edr-module active-charging-service

        [ default ] file [ name file_name ] [ rotation volume volume ] [ rotation
tariff-time minute minute_value hour hour_value ] [ storage-limit limit ] [ reset-
indicator edr-format-name ] [ unique-seq-num ] +

    end

host-select row-precedence

**Applicable Product(s):** GGSN, HA, HSGW, IPSG, PDSN, P-GW, SCM, SAEGW, S-GW

The existing CLI command in the Diameter Host Template Configuration mode is modified to enable the selection of Diameter peer based on the configured prefix/suffix/range values of IMSI or MSISDN of subscriber. This configuration change allows the overlapping range of IMSI or MSISDN values. PCRF peer selection is based on the first match of prefix/suffix/range on row precedence priorities.

With this feature being turned on, the primary and the secondary hosts configured can be picked up in an active standby mode or in round robin fashion.

configure

    diameter-host-template template_name

        host-select row-precedence precedence table { { range-table { 1 | 2 } { imsi-based
{ [ prefix | suffix ] imsi-value [ to imsi-value ] } | msisdn-based { [ prefix | suffix ]
msisdn-value [ to msisdn-value ] } } host host_name [ realm realm_id ] [ secondary host
sec_host_name realm sec_realm_id ] algorithm { active-standby | round-robin } } } [ -
noconfirm ]

        no host-select row-precedence precedence table { 1 | 2 | range-table { 1 | 2 } } [
-noconfirm ]

    end

host-select table

**Applicable Product(s):** GGSN, HA, HSGW, IPSG, PDSN, P-GW, SCM, SAEGW, S-GW

The existing CLI command in the Diameter Host Template Configuration mode is modified to enable the selection of Diameter peer based on the configured prefix/suffix/range values of IMSI or MSISDN of subscriber.

Configuring this command enables activating the configured IMSI or MSISDN table for peer selection.

configure

    diameter-host-template template_name

        host-select table { 1 | 2 | range-table { 1 | 2 } } algorithm { ip-address-modulus
[ prefer-ipv4 | prefer-ipv6 ] | msisdn-modulus | round-robin }

        no host-select table
AAA Changes in Release 15.0

AAA Enhancements for September 30, 2013

logging disable

**Applicable Product(s):** GGSN, HA, HSGW, IPSG, MME, PDSN, P-GW, S-GW

This command enables/disables the logging of the specified event ID or range of IDs. This command has been enhanced to support additional event IDs ranging from 204900 to 204999 for RLF related logging.

```config
logging disable eventid id [ to to_id ]
no logging disable eventid id [ to to_id ]
end
```

logging filter

**Applicable Product(s):** GGSN, HA, HSGW, IPSG, MME, PDSN, P-GW, S-GW

A new facility rlf has been added to this command to enable RLF feature for throttling and rate control.

```config
logging filter active facility rlf level { critical | error | warning | unusual | info | trace | debug }
```

**Important:** Rate Limiting Function (RLF) 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.

msg-type

**Applicable Product(s):** GGSN, HA, HSGW, IPSG, PDSN, P-GW, S-GW

A new optional keyword `retry-server-on-event` has been added to enable reconnecting with PCRF server on update and termination requests or re-authorization from server, for failure-handling CONTINUE sessions.

```config
failure-handling-template template_name
msg-type credit-control-update failure-type any action continue retry-server-on-event
no msg-type credit-control-update failure-type any
end
```

msg-type

**Applicable Product(s):** GGSN, HA, HSGW, IPSG, PDSN, P-GW, S-GW

A keyword option “without-term-req” to retry-and-terminate and terminate failure-handling action in failure handling template configuration has been added to control sending of CCR-T request message when the call terminates.

```config
```
failure-handling-template template_name

msg-type { any | authentication info request | authorization-request | check-identity-request | credit-control-initial | credit-control-terminate | credit-control-update | eap-request | eap-termination-request | notify-request | profile-update-request | purge-ue-request | update-location-request | user-data-request } failure-type { any | diabase-error | diameter result-code { any-error | result-code [ to end-result-code ] } | diameter exp-result-code { any-error | result-code [ to end-result-code ] } | resp-timeout | tx-expiry } action { retry-and-terminate [ without-term-req ] | terminate [ without-term-req ] }

no msg-type { any | authentication info request | authorization-request | check-identity-request | credit-control-initial | credit-control-terminate | credit-control-update | eap-request | eap-termination-request | notify-request | profile-update-request | purge-ue-request | update-location-request | user-data-request } failure-type { any | diabase-error | diameter result-code { any-error | result-code [ to end-result-code ] } | diameter exp-result-code { any-error | result-code [ to end-result-code ] } | resp-timeout | tx-expiry }

end

p-cscf table

Applicable Product(s): GGSN, P-GW, SAEGW
This command is enhanced to include a new keyword “weight” allowing the user to configure and add weight to each row in the p-cscf table. The rows are selected based on weighted round-robin. That is, the row with higher weight parameter is selected more number of times than the row with less number of weights.

Within the IMS Authorization configuration, the P-CSCF address is selected based on round robin fashion. This feature allows the customer to perform P-CSCF selection based on weight factor.

configure

context context_name

ims-auth-service service_name

p-cscf table { 1 | 2 } row-precedence precedence_value { address ipv4_address | ipv6-address ipv6_address } [ secondary { address ipv4_address | ipv6-address ipv6_address } ] [ weight value ]

no p-cscf table { 1 | 2 } row-precedence precedence_value

end

peer

Applicable Product(s): GGSN, MME, P-GW
A new keyword “rlf-template” has been added to this command to enable RLF feature and associate the RLF template with the peer for throttling and rate control.

configure

context context_name
diameter endpoint endpoint_name

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

end

Important: Rate Limiting Function (RLF) 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.

rule-variable

Applicable Product(s): GGSN, P-GW
An optional filter “length” is supported for HTTP URL and User-Agent rule variables which when added will allow the user to configure the length from 1 to 255.

configure

require active charging

active-charging service service_name

edr-format format_name

rule-variable http url length size priority priority

rule-variable http user-agent length size priority priority

end

servers-unreachable

Applicable Product(s): GGSN, HA, IPSG, PDSN, P-GW
This command is enhanced to include a new keyword “result-code” allowing the user to configure error result codes that will trigger entering assume positive mode on the fly for CCR-Initial and CCR-Update messages. CCR-Terminate message is currently not supported.

configure

require active-charging

active-charging service service_name

credit-control

servers-unreachable { behavior-triggers { initial-request | update-request } result-code { any-error | result-code [ to end-result-code ] } }

no servers-unreachable behavior-triggers { initial-request | update-request } result-code { any-error | result-code [ to end-result-code ] }
To maintain backward compatibility i.e. in case of no servers unreachable behavior triggers configured for error result codes, the default hard coded values are applicable.

**show bulkstats variables**

**Applicable Product(s):** GGSN, MME, P-GW

The existing command in the Exec mode has been enhanced to support new schema “rlf” to collect all aggregated information for RLF context statistics.

```
show bulkstats variables rlf [ obsolete ] [ | { grep grep_options | more } ]
```

**show bulkstats variables**

**Applicable Product(s):** GGSN, MME, P-GW

The existing command in the Exec mode has been enhanced to support new schema “rlf-detailed” to collect all detailed instance level information for RLF context statistics.

```
show bulkstats variables rlf-detailed [ obsolete ] [ | { grep grep_options | more } ]
```

**show ims-authorization service name**

**Applicable Product(s):** SAEGW

This existing command in the Exec mode has been enhanced to support new keyword options to collect all P-CSCF server information or specific server information based on the parameters set in the request data. The statistics will be collected on a per IMS Authorization service per P-CSCF server.

```
show ims-authorization service name service_name p-cscf { all | ip-address ipv4/ipv6_address [ | { grep grep_options | more } ]
```

**show variables**

**Applicable Product(s):** GGSN, MME, P-GW

This command has been enhanced to support new schema “rlf” to collect all aggregated information for RLF context statistics.

```
configure

   bulkstats mode

   show variables rlf [ obsolete ]

end
```

**show variables**

**Applicable Product(s):** GGSN, MME, P-GW

This command has been enhanced to support new schema “rlf-detailed” to collect all detailed instance level information for RLF context statistics.

```
configure
```
AAA Changes in Release 15.0

bulkstats mode
    show variables rlf-detailed [ obsolete ]
end

udr trigger

Applicable Product(s): PDSN
This command is used to generate UDR at the configured tariff time. This keyword “tariff-time” allows to configure tariff time trigger to close ongoing UDR buckets and save all data traffic up to tariff time in a single UDR file.
By default, this CLI keyword is disabled.

config
    require active-charging
    active-charging service service_name
    rulebase <rulebase_name>
    udr trigger tariff-time minute minutes hour hours
end

Deprecated Diameter Commands

This section identifies deprecated Diameter commands that are no longer supported in release 15.0.
None for this release.

Diameter Attribute Changes

This section identifies Diameter attribute changes available in release 15.0.

Important: For more information regarding Diameter attributes in this section, refer to the AAA Interface Administration and Reference for this release. For information regarding customer-specific Diameter dictionaries and attributes, contact your account representative.

New Diameter Attributes

This section identifies new Diameter attributes available in release 15.0.
The following attributes are new in this release:
- CLR-Flags
- Charging-Correlation-Indicator
- DEA-Flags
- PUR-Flags
- UE-SRVCC-Capability
Modified Diameter Attributes

This section identifies Diameter attributes modified in release 15.0.

The following attributes have been modified in this release:

- 3GPP-Trigger-Type – A new enumerated value 5 “CHANGE_IN_TIMEZONE” is supported.
- Abort-Cause – A new enumerated value 4 “SPONSORED_DATA_CONNECTIVITY_DISALLOWED” is supported.
- Event-Trigger – The following new enumerated values are supported:
  - 28 - CHARGING_CORRELATION_EXCHANGE
  - 29 - APN_AMBR_MODIFICATION_FAILURE
  - 44 - SERVICE_FLOW_DETECTION
  - 2003 - TETHERING_FLOW_DETECTED
- Experimental-Result-Code – The following new enumerated values are supported:
  - 4199 - DIAMETER_PCRF_TOO_BUSY
  - 5066 - UNAUTHORIZED_NON_EMERGENCY_SESSION
  - 5067 - UNAUTHORIZED_SPONSORED_DATA_CONNECTIVITY
- Reporting-Level – A new enumerated value 2 “SPONSORED_CONNECTIVITY_LEVEL” is supported.
- Requested-Action – A new enumerated value 4 “LOCATION_UPDATE” is supported.
- Rule-Failure-Code – The following new enumerated values are supported:
  - 12 - INCORRECT_FLOW_INFORMATION
  - 13 - PS_TO_CS_HANOVER
  - 15 - NO_BEARER_BOUND
- Trigger-Type – A new enumerated value 5 “CHANGE_IN_UE_TIMEZONE” is supported.

Deprecated Diameter Attributes

This section identifies deprecated Diameter dictionaries that are no longer supported in release 15.0.

None for this release.

Diameter Performance Indicator Changes

This section identifies Diameter performance indicator changes available in release 15.0.

New Diameter Bulk Statistics

This section identifies new Diameter bulk statistics available in release 15.0.

New in the Diameter Authentication Schema

The following bulkstatistics variables are newly added to this schema to support result code based bulkstatistics for S6b/STa Interface.
• diameter-auth-msg-multiround
• diameter-auth-msg-success
• diameter-auth-msg-err-protocol
• diameter-auth-msg-err-transient
• diameter-auth-msg-err-permanent
• diameter-auth-msg-err-other

New in the DPCA Schema

The following are the bulkstatistic variables that are available in this schema.

• server-type
• active-sessions

New in the IMSA Schema

The following are the new bulkstatistic variables that are available in this schema.

• dpca-fallback-sessions
• dpca-msg-sgw-restore-rar-reject
• dpca-msg-sgw-restore-reval-timeout
• dpca-msg-sgw-restore-pending-updates
• dpca-ccfh-retry-and-term-wo-ccrt
• dpca-ccfh-terminate-wo-ccrt
• dpca-imsa-msg-success
• dpca-imsa-msgerrproto
• dpca-imsa-msgerr-transfailure
• dpca-imsa-msgerr-permfailure
• dpca-imsa-msgerr-otherrescode
• dpca-imsa-tethering-flow-detected

New in the RLF Schema

This schema is new in this release. The following are the bulkstatistic variables that are available in this schema.

• rlf-ctx-name
• rlf-template-name
• rlf-cfg-tps
• rlf-state
• rlf-storage
• rlf-direction
• rlf-tot-active-time
• rlf-curr-queue-size
• rlf-avg-tps
• rlf-trend-tps
• rlf-10sec-avg-tps
• rlf-30sec-avg-tps
• rlf-60sec-avg-tps
• rlf-5min-avg-tps
• rlf-10min-avg-tps
• rlf-avg-bypass-tps
• rlf-10sec-avg-bypass-tps
• rlf-30sec-avg-bypass-tps
• rlf-60sec-avg-bypass-tps
• rlf-5min-avg-bypass-tps
• rlf-10min-avg-bypass-tps
• rlf-threshold-exceeded
• rlf-queued
• rlf-dropped
• rlf-directly-sent
• rlf-queue-bypassed
• rlf-send-msg-cb-failed
• rlf-status-update-cb-failed

New in the RLF-Detailed Schema

This schema is new in this release. The following are the bulkstatistic variables that are available in this schema.

• rlf-ctx-name
• rlf-template-name
• rlf-instance-num
• rlf-cfg-tps
• rlf-state
• rlf-curr-queue-size
• rlf-avg-tps
• rlf-trend-tps
• rlf-min-achieved-tps
• rlf-max-achieved-tps
Modified Diameter Bulk Statistics

This section identifies Diameter bulk statistics modified in release 15.0. None for this release.

Deprecated Diameter Bulk Statistics

This section identifies deprecated Diameter bulk statistics that are no longer supported in release 15.0. None for this release.

New Diameter Output Fields and Counters

This section identifies new Diameter show command output fields and counters available in release 15.0.

**show active-charging charging-action**

The following field has been added to the output of this command to indicate if the selective TFT suppression feature is enabled or disabled for all bearers including default and dedicated bearers.

- TFT updates to UE

**show active-charging rulebase name**

The following field has been added to the output of this command to indicate if the RAN Bandwidth Optimization feature is enabled or disabled.

- Ran Bandwidth Optimization

The following field has been added to the output of this command to indicate if the selective TFT suppression feature is enabled or disabled for the default bearer.

- TFT updates to UE for default bearer

**show active-charging service statistics**

**Applicable Product(s):** GGSN, HA, IPSG, PDSN, P-GW

The following fields have been added to support system level statistics to display the number of dropped uplink/downlink bytes/packets.

- Credit-Control Group Statistics
  - CC Dropped Uplink Packets
  - CC Dropped Uplink Bytes
  - CC Dropped Downlink Packets
  - CC Dropped Downlink Bytes

**show active-charging sessions full all**

**Applicable Product(s):** GGSN, P-GW

This command displays the statistics for Active Charging Service (ACS) sessions. In this release, the output of this CLI command has been modified to include the new reporting level “SPONSORED_CONNECTIVITY_LEVEL” and two
new AVPs “Sponsor-Identity” and “Application-Service-Provider-Identity” introduced as part of the Sponsored data connectivity feature.

If the PCRF sends these new AVPs during the dynamic rule installation/modification, these AVPs are indicated in the output of “show active-charging sessions full all” command irrespective of the reporting level.

For more information on this feature, refer to the Support for Sponsor Identity over Gx section.

```
show active-charging sessions [ full [ wide ] | summary ] [ filter_keyword + ] + [ all ] [ | { grep grep_options | more } ]
```

**show active-charging subsystem all**

**Applicable Product(s):** GGSN, HA, IPSG, PDSN, P-GW

The following fields have been added to support system level statistics to display the number of dropped uplink/downlink bytes/packets.

- CC Dropped Uplink Packets
- CC Dropped Uplink Bytes
- CC Dropped Downlink Packets
- CC Dropped Downlink Bytes

**show bulkstats variables**

**Applicable Product(s):** SAEGW

This command displays the bulkstatistics information corresponding to specified schema name and variables. In this release, a few bulkstatistic variables are supported in the DPCA schema.

For the complete list of bulkstatistic variables supported, refer to the New Diameter Bulk Statistics section.

```
show bulkstats variables dpca [ obsolete ] [ | { grep grep_options | more } ]
```

**show bulkstats variables**

**Applicable Product(s):** GGSN, HA, HSGW, IPSG, PDSN, P-GW, S-GW

This command displays the bulkstatistics information corresponding to specified schema name and variables. In this release, a few bulkstatistic variables are supported in the IMSA schema.

For the complete list of bulkstatistic variables supported, refer to the New Diameter Bulk Statistics section.

```
show bulkstats variables imsa [ obsolete ] [ | { grep grep_options | more } ]
```

**show diameter peers full all**

**Applicable Product(s):** GGSN, HA, P-GW

The following field has been added to support local-policy fallback scenario.

- Peer Backoff Timer State

**show diameter aaa-statistics**

**Applicable Product(s):** P-GW
The following fields have been added to the output of this command to collect the result code based statistics for S6b/STa interface.

- Result Code Stats
  - Result Code 1xxx
  - Result Code 2xxx
  - Result Code 3xxx
  - Result Code 4xxx
  - Result Code 5xxx
  - Other Result Code

show diameter statistics

Applicable Product(s): GGSN, HA, P-GW

The following fields have been added to support local-policy fallback scenario.

- Peer Backoff Timer
  - Start-count
  - Stop-count

show hss-peer-service service name

Applicable Product(s): SGSN

A new parameter has been added to indicate the configured release compliance of the Standard dictionary used for HSS Peer Service.

- Update-Dictionary-Avps

show ims-authorization policy-control statistics

Applicable Product(s): GGSN, HA, HSGW, IPSG, PDSN, P-GW, S-GW

The following fields have been added to display statistics based on the error result codes.

- CCA Result Code Stats
  - Result Code 2xxx
  - Result Code 3xxx
  - Result Code 4xxx
  - Result Code 5xxx
  - Other Result Code

The following fields have been added to display the statistics introduced in support of the S-GW restoration feature.

- SGW Restoration
  - RAR Reject
  - Internal Updates Dropped
• Revalidation Timeout
• Pending Updates

The following field has been added to indicate the number of sessions that successfully fallback to PCRF after being with local-policy.

• Total Fallback Sessions

The following fields have been added to display the statistics introduced in support of PCRF reconnection when the failure handling action “continue” is applied.

• DPCA FH Retry Server On Event
  • CCR-Update
  • CCR-Terminate
  • RAR
• FH Behavior
  • Retry Server On Event

The following fields have been added under FH Behavior category to control sending of CCR-T to PCRF when the call terminates.

• Termination
  • Retry Term without CCRT
  • Terminate without CCRT

**show ims-authorization service name**

**Applicable Product(s):** GGSN, HA, HSGW, IPSG, PDSN, P-GW, S-GW

The following field has been added to support Diameter peer selection at Diabase in all failure scenarios.

• Endpoint Peer Select

The following field has been added to support encoding and sending of Supported-Features AVP with Sponsor Identity.

• Supported Features

The following field has been added under P-CSCF Discovery category in the output of this command to support weight-based P-CSCF server selection.

• Weight

**show ims-authorization sessions full all**

**Applicable Product(s):** GGSN, P-GW

The following field has been added to display the supported features that are actually applied to the session after negotiation with PCRF.

• Negotiated Supported Features

**show ims-authorization service statistics**

**Applicable Product(s):** GGSN, HA, HSGW, IPSG, PDSN, P-GW, S-GW

The following fields have been added to support local-policy fallback scenario.
• Local-Fallback
  • CCRU received
  • RAR received

The following fields have been added to support statistics of APN_AMBR_MODIFICATION_FAILURE and DEFAULT_EPS_BEARER_QOS_MODIFICATION_FAILURE event triggers in EPS 3.0:
  • APN AMBR Modification Failure
  • Def EPSBearer QOS Mod Failure

**show ims-authorization service statistics name**

**Applicable Product(s):** GGSN, HA, HSGW, IPSG, PDSN, P-GW, S-GW

The following fields have been added to support Diameter peer selection at Diabase in all failure scenarios.
  • Endpoint Peer Select
    • Host Select Failure
    • Inactive Host

The following field has been added to support Charging Correlation Exchange over Gx interface.
  • Chrg Correlation Exchange

The following field has been added to support the addition of new event trigger for reporting tethered traffic.
  • Tethering Flow Detected

**Important:** This field is customer-specific. For more information, contact your local Cisco account representative.

**show local-policy statistics all**

**Applicable Product(s):** GGSN, HA, P-GW

The following fields have been added to the category “Action Statistics” that appears in the output of this command. These fields have been added to support retry attempts to connect with PCRF in the event of CCR failure.
  • Reconnect to Server
  • Reconnect to Server Failure
  • Reconnect to Server Success

The following field has been added to perform a rule matching based on the PDN Type.
  • PDN Type

**show variables**

**Applicable Product(s):** SAEGW

This command displays the bulkstatistics information corresponding to specified schema name and variables. In this release, a few bulkstatistic variables are supported in the DPCA schema.

For the complete list of bulkstatistic variables supported, refer to the New Diameter Bulk Statistics section.
configure

   bulkstats mode

   show variables dpca [ obsolete ]

   end

show variables

Applicable Product(s): GGSN, HA, HSGW, IPSG, PDSN, P-GW, S-GW

This command displays the bulkstatistics information corresponding to specified schema name and variables. In this release, a few bulkstatistic variables are supported in the IMSA schema.

For the complete list of bulkstatistic variables supported, refer to the New Diameter Bulk Statistics section.

configure

   bulkstats mode

   show variables imsa [ obsolete ]

   end

Modified Diameter Output Fields and Counters

This section identifies Diameter show command output fields and counters modified in release 15.0.

show ims-authorization service name

Applicable Product(s): GGSN, HA, HSGW, IPSG, PDSN, P-GW, S-GW

The “Reauth Trigger” field in the output of this command displays Charging-Correlation-Exchange if this trigger is configured.

show ims-authorization sessions full all

Applicable Product(s): GGSN, HA, HSGW, IPSG, PDSN, P-GW, S-GW

The “Event Triggers” field in the output of this command displays Charging-Correlation-Exchange if this trigger is configured.

show active-charging sessions full all

Applicable Product(s): GGSN, HA, HSGW, IPSG, PDSN, P-GW, S-GW

The output of this command has been modified to display “Negotiated-QoS” info instead of “Authorized-QoS” information to support sending QoS-Info AVP always in the CCR-U messages.

Deprecated Diameter Output Fields and Counters

This section identifies deprecated Diameter show command output fields and counters that are no longer supported in release 15.0.

None for this release.
RADIUS Accounting Management Changes as of September 30, 2013

This section provides information on RADIUS accounting management changes available in release 15.0.

RADIUS Feature Changes

This section identifies RADIUS features changes available in release 15.0.

New RADIUS Features

This section identifies new RADIUS features available in release 15.0.

None for this release.

Modified RADIUS Features

This section identifies RADIUS features modified in release 15.0.

Dictionary Changes for BSID Information in Online RADIUS Message

Applicable Product(s): PDSN

With this enhancement, online RADIUS access request message includes the 3GPP-BSID RADIUS attribute. This attribute is added only to custom4 and custom55 RADIUS dictionaries.

Enhancements to “show configuration errors” for misconfigurations in AAA

Applicable Product(s): GGSN, P-GW

The CLI command “show configuration errors” has been modified to accommodate new error messages related to AAA/APN configurations. The main purpose of this enhancement is to display configuration errors. This enhancement checks all AAA CLI commands and if there is mismatch, show configuration errors is flagged in the show subscriber details command.

With the current enhancement, this command additionally displays error/warning message if –

• a AAA group is not defined in the same context as APN
• the charging-agent defined in a GTPP group is not assigned to any interface and if it's a non-default group
• the charging-agent is invalid and it is a default group

Configuration Support for RADIUS Attributes

Applicable Product(s): GGSN, P-GW

A new CLI is introduced to control the configuration of the following RADIUS attributes.

• Service-Type
• Framed-IP-Address
• Framed-IPv6-Prefix
• Acct-Session-Id
• CHAP-Challenge
• NAS-Port-Type
• Class
• Acct-Status-Type
• Acct-Authentic
• Username
• Acct-Delay-Time
• 3GPP-Session-Stop-Indicator
• nas-ip-address
• nas-identifier

With this feature, the customers can either enable or disable these attributes as needed.

RADIUS Command Changes

This section identifies RADIUS command changes available in release 15.0.

**Important:** For more information regarding commands in this section, refer to the *Command Line Interface Reference* for this release.

New RADIUS Commands

This section identifies new RADIUS commands available in release 15.0.

None for this release.

Modified RADIUS Commands

This section identifies RADIUS commands modified in release 15.0.

**radius attribute accounting**

**Applicable Product(s):** GGSN, P-GW

This command enables the listed RADIUS accounting attributes, provided they are supported in the configured RADIUS dictionary.

```
config
  context context_name
    aaa group group_name
      [ no ] radius attribute accounting { service-type | framed-ip-address | framed-ipv6-prefix | acct-cession-id | nas-port-type | class | acct-status-type | acct-authentic | username | acct-delay-time | 3gpp-session-stop-indicator | nas-ip-address | nas-identifier }
      default radius attribute accounting
```
By default, all of the attributes are enabled.

**radius attribute authentication**

This command enables the listed RADIUS authentication attributes, provided they are supported in the configured RADIUS dictionary.

```plaintext
config
case context_name

aaa group group_name

[no] radius attribute authentication { service-type | framed-ip-address | framed-ipv6-prefix | chap-challenge | nas-port-type | username | nas-ip-address | nas-identifier }

default radius attribute authentication
end
```

By default, all of the attributes are enabled.

**Deprecated RADIUS Commands**

This section identifies deprecated RADIUS commands that are no longer supported in release 15.0.

None for this release.

**RADIUS Attribute Changes**

This section identifies RADIUS attribute changes available in release 15.0.

> **Important**: For more information regarding RADIUS dictionaries and attributes in this section, refer to the *AAA Interface Administration and Reference* for this release. For information regarding customer-specific RADIUS dictionaries and attributes, contact your account representative.

**New RADIUS Attributes**

This section identifies new RADIUS attributes available in release 15.0.

The following attributes are new in this release:

- Service-Selection
- SN-Congestion-Mgmt-Policy
- SN-Customer-ID
- SN-FMC-Location
- SN-LBO-Acct-IN-Pkts
- SN-LBO-Acct-Out-Pkts
• SN-LBO-Acct-IN-Octets
• SN-LBO-Acct-Out-Octets
• SN-WSG-MIP-Required
• SN-WSG-MIP-Release-TIA
• SN-WSG-MIP-Simple-IP-Fallback

**Important:** Attribute descriptions for new RADIUS attributes are located in the *AAA Interface Administration and Reference* for this release.

## Modified RADIUS Attributes

This section identifies RADIUS attributes modified in release 15.0.

The following attributes have been modified in this release:

- 3GPP2-PMIP-IPv4Session-Info – Added the following subattributes “PMN-LMA-KEY” and “PMN-LMA-SPI”
- SN-Disconnect-Reason – The following new enumerated values are supported:
  - NAT-Pool-BusyOut-Or-Pend-Delete = 536
  - Invalid-APN = 537
  - srvcc-ps-to-cs-handover = 538
  - henbgw-mme-slap-reset-reced = 539
  - henbgw-henb-slap-reset-reced = 540
  - henbgw-mme-sctp-conn-down = 541
  - henbgw-henb-sctp-conn-down = 542
  - henbgw-handoff-complete = 543
  - henbgw-handover-failed = 544
  - henbgw-mme-error-indication = 545
  - henbgw-henb-error-indication = 546
  - henbgw-henb-initiated-release = 547
  - henbgw-mme-initiated-release = 548
  - henbgw-duplicate-session = 549
  - Transport-mismatch-with-PGW = 550
  - icsr-ipsec-chkpt-failed = 551
  - sgsn-dbr-cause-isr-deact-detach = 552
- SN1-Disconnect-Reason – The following new enumerated values are supported:
  - NAT-Pool-BusyOut-Or-Pend-Delete = 536
  - Invalid-APN = 537
  - srvcc-ps-to-cs-handover = 538
AAA Changes in Release 15.0

AAA Enhancements for September 30, 2013

- henbgw-mme-s1ap-reset-reced = 539
- henbgw-henb-s1ap-reset-reced = 540
- henbgw-mme-sctp-conn-down = 541
- henbgw-henb-sctp-conn-down = 542
- henbgw-handoff-complete = 543
- henbgw-handover-failed = 544
- henbgw-mme-error-indication = 545
- henbgw-henb-error-indication = 546
- henbgw-henb-initiated-release = 547
- henbgw-mme-initiated-release = 548
- henbgw-duplicate-session = 549
- Transport-mismatch-with-PGW = 550
- icsr-ipsec-chkpt-failed = 551
- sgsn-dbr-cause-isr-deact-detach = 552

- SN-QoS-Negotiated – The maximum length for this attribute is changed from 20 to 28.
- SN-Service-Type – Added new enumerated values WSG and SAMOG
- SN1-Service-Type – Added new enumerated values WSG and SAMOG

Deprecated RADIUS Attributes

This section identifies deprecated RADIUS attributes that are no longer supported in release 15.0.

None for this release.

RADIUS Performance Management Changes

This section identifies RADIUS performance management changes available in release 15.0.

Important: For more information regarding bulk statistics in this section, refer to the Statistics and Counters Reference for this release. For more information regarding commands in this section, refer to the Command Line Interface Reference for this release.

New RADIUS Bulk Statistics

This section identifies new RADIUS bulk statistics available in release 15.0.

None for this release.

Modified RADIUS Bulk Statistics

This section identifies RADIUS bulk statistics modified in release 15.0.

None for this release.
**Deprecated RADIUS Bulk Statistics**

This section identifies deprecated RADIUS bulk statistics that are no longer supported in release 15.0.

None for this release.

**New RADIUS Output Fields and Counters**

This section identifies new RADIUS show command output fields and counters available in release 15.0.

None for this release.

**Modified RADIUS Output Fields and Counters**

This section identifies RADIUS show command output fields and counters modified in release 15.0.

None for this release.

**Deprecated RADIUS Output Fields and Counters**

This section identifies deprecated RADIUS show command output fields and counters that are no longer supported in release 15.0.

None for this release.
Chapter 2
ADC Changes in Release 15.0

This chapter identifies features and functionality added to, modified for, or deprecated from 15.0 ADC software releases.
ADC Enhancements for February 28, 2014

Important: The changes identified in this section pertain to the ADC plugin release slated for February 28, 2014.

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 *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.

CSCu125213 - Add Support for BBM app in iOS and Android

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

**Feature Changes**

**Support for BBM Application Detection**

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

**Command Changes**

**p2p-detection protocol**

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

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

```
configure

active-charging service service_name

[ no ] p2p-detection protocol bbm

end
```

**p2p protocol**

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

With this release, the BBM protocol is supported.

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

clear active-charging analyzer statistics
This command enables detection of specific P2P protocols for charging purposes.
With this release, the BBM protocol is supported.
clear active-charging analyzer statistics [ name protocol_name ] [ | { grep grep_options | more } ]

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

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

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

Performance Indicator Changes

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

- p2p-bbm-group
- p2p-bbm-uplnk-bytes
- p2p-bbm-dwlnk-bytes
• p2p-bbm-uplnk-pkts
• p2p-bbm-dwnlnk-pkts
• p2p-bbm-duration
• p2p-bbm-unclassified-uplnk-bytes
• p2p-bbm-unclassified-dwnlnk-bytes
• p2p-bbm-unclassified-uplnk-pkts
• p2p-bbm-unclassified-dwnlnk-pkts
• p2p-bbm-unclassified-duration
• p2p-bbm-audio-uplnk-bytes
• p2p-bbm-audio-dwnlnk-bytes
• p2p-bbm-audio-uplnk-pkts
• p2p-bbm-audio-dwnlnk-pkts
• p2p-bbm-audio-duration

show active-charging analyzer statistics name p2p verbose

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

• Bbm:
  • Total Uplink Bytes
  • Total Downlink Bytes
  • Total Uplink Packets
  • Total Downlink Packets

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

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

• Communicator-bbm:
  • Total Uplink Bytes
  • Total Downlink Bytes
  • Total Uplink Packets
  • Total Downlink Packets

show active-charging sessions summary

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

• Current BBM Sessions
• Current BBM UNCLASSIFIED Sessions
• Current BBM AUDIO Sessions
CSCuJ99411 - Support BOX application in ADC

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

Feature Changes

Support for Box Application Detection

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

Command Changes

p2p-detection protocol

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

configure

active-charging service service_name

[ no ] p2p-detection protocol box

end

p2p protocol

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

configure

active-charging service service_name

ruledef ruledef_name

[ no ] p2p protocol box

end

clear active-charging analyzer statistics

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

clear active-charging analyzer statistics [ name protocol_name ] [ | { grep grep_options | more } ]

show active-charging analyzer statistics name p2p

This command displays statistical information for protocol analyzers.
With this release, the box keyword is added to the p2p list:

\[\text{show active-charging analyzer statistics name p2p application p2p_list}\]

\[\text{show active-charging flows type p2p}\]

This command displays the information for the active charging flows.

With this release, the box keyword is added to the p2p list:

\[\text{show active-charging flows type p2p application p2p_list}\]

\[\text{show active-charging sessions summary}\]

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

With this release, the box keyword is added to the p2p list:

\[\text{show active-charging sessions summary type p2p application p2p_list}\]

**Performance Indicator Changes**

**P2P Schema**

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

The following bulk statistics are added to the P2P schema:

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

\[\text{show active-charging analyzer statistics name p2p verbose}\]

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

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

- Box:
  - Total Uplink Bytes
  - Total Downlink Bytes
  - Total Uplink Packets
  - Total Downlink Packets

\[\text{show active-charging analyzer statistics name p2p protocol-group verbose}\]
With this release, the following fields have been added to the output of this command:

- Cloud-box:
  - Total Uplink Bytes
  - Total Downlink Bytes
  - Total Uplink Packets
  - Total Downlink Packets

**show active-charging sessions summary**

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

- Current Box Sessions

**CSCul82621 - Support for Chikka mail and IM in p2p plugin**

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

**Feature Changes**

**Support for Chikka Application Detection**

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

**Command Changes**

**p2p-detection protocol**

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

```
configure

active-charging service service_name

[ no ] p2p-detection protocol chikka

end
```

**p2p protocol**

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

```
configure

active-charging service service_name

ruledef ruledef_name
```
[ no ] p2p protocol chikka

end

clear active-charging analyzer statistics
This command enables detection of specific P2P protocols for charging purposes.
With this release, the Chikka protocol is supported.
clear active-charging analyzer statistics [ name protocol_name ] [ | { grep grep_options | more } ]

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

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

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

Performance Indicator Changes

P2P Schema
New ADC bulk statistics are available in the P2P schema for chikka as part of the plugin. If detection of the Chikka P2P protocol is enabled, bulk statistics for that protocol will be automatically generated using the Dynamic Software Upgrade plugin installed on the chassis.
The following bulk statistics are added to the P2P schema:
• p2p-chikka-group
• p2p-chikka-uplnk-bytes
• p2p-chikka-dwlknk-bytes
• p2p-chikka-uplnk-pkts
• p2p-chikka-dwlknk-pkts
• p2p-chikka-duration
ADC Changes in Release 15.0

ADC Enhancements for February 28, 2014

- p2p-chikka-audio-uplnk-bytes
- p2p-chikka-audio-dwlnk-bytes
- p2p-chikka-audio-uplnk-pkts
- p2p-chikka-audio-dwlnk-pkts
- p2p-chikka-audio-duration

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

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

- Chikka:
  - Total Uplink Bytes
  - Total Downlink Bytes
  - Total Uplink Packets
  - Total Downlink Packets

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

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

- E-Mail-chikka:
  - Total Uplink Bytes
  - Total Downlink Bytes
  - Total Uplink Packets
  - Total Downlink Packets

**show active-charging sessions summary**

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

- Current Chikka Sessions
- Current Chikka Audio Sessions

**CSCul82673 - Support for imgur in p2p plugin**

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

**Feature Changes**

**Support for Imgur Application Detection**

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

p2p-detection protocol

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

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

p2p protocol

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

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

clear active-charging analyzer statistics

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

```
clear active-charging analyzer statistics [ name protocol_name ] [ | { grep grep_options | more } ]
```

show active-charging analyzer statistics name p2p

This command displays statistical information for protocol analyzers. With this release, the imgur keyword is added to the p2p list:

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

show active-charging flows type p2p

This command displays the information for the active charging flows. With this release, the imgur keyword is added to the p2p list:

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

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

With this release, the `imgur` keyword is added to the p2p list:

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

Performance Indicator Changes

P2P Schema

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

The following bulk statistics are added to the P2P schema:

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

show active-charging analyzer statistics name p2p verbose

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

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

- Imgur:
  - Total Uplink Bytes
  - Total Downlink Bytes
  - Total Uplink Packets
  - Total Downlink Packets

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

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

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

show active-charging sessions summary
With this release, the following fields have been added to the output of this command:

- Current Imgur Sessions

**CSCul82626 - Support for Oist in p2p plugin**

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

**Feature Changes**

**Support for Oist Application Detection**

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

**Command Changes**

**p2p-detection protocol**

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

```bash
configure

active-charging service service_name

[ no ] p2p-detection protocol oist

end
```

**p2p protocol**

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

```bash
configure

active-charging service service_name

ruledef ruledef_name

[ no ] p2p protocol oist

end
```

**clear active-charging analyzer statistics**

This command enables detection of specific P2P protocols for charging purposes. With this release, the Oist protocol is supported.
clear active-charging analyzer statistics [ name protocol_name ] [ | { grep grep_options | more } ]

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

show active-charging analyzer statistics name p2p application p2p_list

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

show active-charging flows type p2p application p2p_list

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

show active-charging sessions summary type p2p application p2p_list

Performance Indicator Changes

P2P Schema

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

The following bulk statistics are added to the P2P schema:

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

show active-charging analyzer statistics name p2p verbose
This command displays Active Charging protocol analyzer statistics for the P2P protocol analyzer.
With this release, the following fields have been added to the output of this command:

- Oist:
  - Total Uplink Bytes
show active-charging analyzer statistics name p2p protocol-group verbose

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

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

show active-charging sessions summary

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

- Current Oist Sessions

CSCul82671 - Support for regram in p2p plugin

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

Feature Changes

Support for Regram Application Detection

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

Command Changes

p2p-detection protocol

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

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

configure

active-charging service service_name

[ no ] p2p-detection protocol regram

end

p2p protocol
This command enables detection of specific P2P protocols for charging purposes.
With this release, the Regram protocol is supported.

```
configure

active-charging service service_name

ruledef ruledef_name

[ no ] p2p protocol regram

end
```

```
clear active-charging analyzer statistics
```

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

```
clear active-charging analyzer statistics [ name protocol_name ] [ | { grep grep_options
| more } ]
```

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

This command displays statistical information for protocol analyzers.
With this release, the `regram` keyword is added to the p2p list:

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

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

This command displays the information for the active charging flows.
With this release, the `regram` keyword is added to the p2p list:

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

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

This command displays statistics for Active Charging Service (ACS) sessions.
With this release, the `regram` keyword is added to the p2p list:

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

**Performance Indicator Changes**

**P2P Schema**

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

The following bulk statistics are added to the P2P schema:
• p2p-regram-group
• p2p-regram-uplnk-bytes
• p2p-regram-dwlnk-bytes
• p2p-regram-uplnk-pkts
• p2p-regram-dwlnk-pkts
• p2p-regram-duration

show active-charging analyzer statistics name p2p verbose

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

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

• Regram:
  • Total Uplink Bytes
  • Total Downlink Bytes
  • Total Uplink Packets
  • Total Downlink Packets

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

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

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

show active-charging sessions summary

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

• Current Regram Sessions

CSCuc72953 - Support for additional P2P protocol in ADC

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

Feature Changes

Support for VChat Application Detection

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

p2p-detection protocol

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

configure

active-charging service service_name

[ no ] p2p-detection protocol vchat
end

p2p protocol

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

configure

active-charging service service_name

ruledef ruledef_name

[ no ] p2p protocol vchat
end

clear active-charging analyzer statistics

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

clear active-charging analyzer statistics [ name protocol_name ] [ | { grep grep_options | more } ]

show active-charging analyzer statistics name p2p

This command displays statistical information for protocol analyzers. With this release, the vchat keyword is added to the p2p list:

show active-charging analyzer statistics name p2p application p2p_list

show active-charging flows type p2p

This command displays the information for the active charging flows. With this release, the vchat keyword is added to the p2p list:

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

This command displays statistics for Active Charging Service (ACS) sessions. With this release, the `vchat` keyword is added to the p2p list:

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

Performance Indicator Changes

P2P Schema

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

The following bulk statistics are added to the P2P schema:

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

show active-charging analyzer statistics name p2p verbose

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

- Vchat:
  - Total Uplink Bytes
  - Total Downlink Bytes
  - Total Uplink Packets
  - Total Downlink Packets

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

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

- Social-nw-videoconf-vchat:
  - Total Uplink Bytes
  - Total Downlink Bytes
  - Total Uplink Packets
  - Total Downlink Packets

show active-charging sessions summary
With this release, the following fields have been added to the output of this command:

- Current Vchat Sessions
ADC Enhancements for December 20, 2013

Important: The changes identified in this section pertain to the ADC plugin release slated for December 20, 2013. For more information regarding features in this section, refer to the ADC Administration Guide dated December 20, 2013.

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 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.

CSCug26539 - Support for JAP in the p2p plugin

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

Feature Changes

Support for JAP Application Detection

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

Command Changes

p2p-detection protocol

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

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

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

p2p protocol

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

With this release, the Jap protocol is supported.
configure

active-charging service service_name

ruledef ruledef_name

[ no ] p2p protocol jap

end

clear active-charging analyzer statistics

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

clear active-charging analyzer statistics [ name protocol_name ] [ | { grep grep_options | more } ]

show active-charging analyzer statistics name p2p

This command displays statistical information for protocol analyzers.
With this release, the jap keyword is added to the p2p list:

show active-charging analyzer statistics name p2p application p2p_list

show active-charging flows type p2p

This command displays the information for the active charging flows.
With this release, the jap keyword is added to the p2p list:

show active-charging flows type p2p application p2p_list

show active-charging sessions summary

This command displays statistics for Active Charging Service (ACS) sessions.
With this release, the jap keyword is added to the p2p list:

show active-charging sessions summary type p2p application p2p_list

Performance Indicator Changes

P2P Schema

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

The following bulk statistics are added to the P2P schema:

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

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

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

- Jap:
  - Total Uplink Bytes
  - Total Downlink Bytes
  - Total Uplink Packets
  - Total Downlink Packets

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

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

- Anonymous-Access-jap:
  - Total Uplink Bytes
  - Total Downlink Bytes
  - Total Uplink Packets
  - Total Downlink Packets

**show active-charging sessions summary**

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

- Current JAP Sessions

**CSCuh57347 - ADC Support Monkey3**

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

**Feature Changes**

**Support for Monkey3 Application Detection**

With this release, the support for detection of traffic originating from the Monkey3 application is added.
Command Changes

p2p-detection protocol

This command enables detection of peer-to-peer (P2P) protocols.
With this release, the monkey3 keyword is added to this command:

```
configure
  active-charging service service_name
  [ no ] p2p-detection protocol monkey3
end
```

p2p protocol

This command enables detection of specific P2P protocols for charging purposes.
With this release, the Monkey3 protocol is supported.

```
configure
  active-charging service service_name
  ruledef ruledef_name
  [ no ] p2p protocol monkey3
end
```

clear active-charging analyzer statistics

This command enables detection of specific P2P protocols for charging purposes.
With this release, the Monkey3 protocol is supported.

```
clear active-charging analyzer statistics [ name protocol_name ] [ | { grep grep_options | more } ]
```

show active-charging analyzer statistics name p2p

This command displays statistical information for protocol analyzers.
With this release, the monkey3 keyword is added to the p2p list:

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

show active-charging flows type p2p

This command displays the information for the active charging flows.
With this release, the monkey3 keyword is added to the p2p list:

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

This command displays statistics for Active Charging Service (ACS) sessions. With this release, the `monkey3` keyword is added to the p2p list:

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

Performance Indicator Changes

P2P Schema

New ADC bulk statistics are available in the P2P schema for monkey3 as part of the plugin. If detection of the Monkey3 P2P protocol is enabled, bulk statistics for that protocol will be automatically generated using the Dynamic Software Upgrade plugin installed on the chassis.

The following bulk statistics are added to the P2P schema:

- p2p-monkey3-group
- p2p-monkey3-uplnk-bytes
- p2p-monkey3-dwlnk-bytes
- p2p-monkey3-uplnk-pkts
- p2p-monkey3-dwlnk-pkts
- p2p-monkey3-duration

show active-charging analyzer statistics name p2p verbose

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

- Monkey3:
  - Total Uplink Bytes
  - Total Downlink Bytes
  - Total Uplink Packets
  - Total Downlink Packets

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

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

- Streaming-monkey3:
  - Total Uplink Bytes
  - Total Downlink Bytes
  - Total Uplink Packets
  - Total Downlink Packets

show active-charging sessions summary
With this release, the following fields have been added to the output of this command:

- Current Monkey3 Sessions

**CSCui57348 - Add Support for Facebook Voice in iOS and Android Apps**

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

**Feature Changes**

**Support for Detection of Facebook VoIP Calls**

With this release, Facebook VoIP calls over iOS and Android devices will be detected and classified under the facebook audio sub-classification.

**Command Changes**

`show active-charging flows`

This command displays the information for the active charging flows.

With this release, the `audio` keyword is added for the facebook p2p protocol:

`show active-charging flows [ full ] type p2p application facebook traffic-type { audio | unclassified }`

`show active-charging sessions`

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

With this release, the `audio` keyword is added for the facebook p2p protocol:

`show active-charging sessions [ full ] type p2p application facebook traffic-type { audio | unclassified }`

**Performance Indicator Changes**

**show active-charging sessions**

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

- Current facebook Sessions
show active-charging analyzer statistics

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

- Facebook unclassified:
  - Total Uplink Bytes
  - Total Downlink Bytes
  - Total Uplink Pkts
  - Total Downlink Pkts
- Facebook audio:
  - Total Uplink Bytes
  - Total Downlink Bytes
  - Total Uplink Pkts
  - Total Downlink Pkts

CSCui93029 - Apple Maps support in P2P Protocol

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

Feature Changes

Support for Apple Maps Application Detection

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

Command Changes

p2p-detection protocol

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

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

configure

    active-charging service service_name

    [ no ] p2p-detection protocol applemaps

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

```
configure

   active-charging service service_name

   ruledef ruledef_name

       [ no ] p2p protocol applemaps

   end

```

**clear active-charging analyzer statistics**

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

```
clear active-charging analyzer statistics [ name protocol_name ] [ | { grep grep_options | more } ]
```

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

This command displays statistical information for protocol analyzers.
With this release, the applemaps keyword is added to the p2p list:

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

**show active-charging flows type p2p**

This command displays the information for the active charging flows.
With this release, the applemaps keyword is added to the p2p list:

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

**show active-charging sessions summary**

This command displays statistics for Active Charging Service (ACS) sessions.
With this release, the applemaps keyword is added to the p2p list:

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

### Performance Indicator Changes

### P2P Schema

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

The following bulk statistics are added to the P2P schema:
- p2p-applemaps-group
- p2p-applemaps-uplnk-bytes
- p2p-applemaps-dwlnk-bytes
- p2p-applemaps-uplnk-pkts
- p2p-applemaps-dwlnk-pkts
- p2p-applemaps-duration

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

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

- Applemaps:
  - Total Uplink Bytes
  - Total Downlink Bytes
  - Total Uplink Packets
  - Total Downlink Packets

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

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

- Untagged-applemaps:
  - Total Uplink Bytes
  - Total Downlink Bytes
  - Total Uplink Packets
  - Total Downlink Packets

**show active-charging sessions summary**

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

- Current Applemaps Sessions

**CSCuj44380 - Support yahoo mail in P2P detection**

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

**Feature Changes**

**Support for Yahoo Mail Application Detection**

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

p2p-detection protocol

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

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

```
configure

active-charging service service_name

[ no ] p2p-detection protocol yahoomail

end
```

p2p protocol

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

With this release, the Yahoo Mail protocol is supported.

```
configure

active-charging service service_name

ruledef ruledef_name

[ no ] p2p protocol yahoomail

end
```

clear active-charging analyzer statistics

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

With this release, the Yahoo Mail protocol is supported.

```
clear active-charging analyzer statistics [ name protocol_name ] [ | { grep grep_options | more } ]
```

show active-charging analyzer statistics name p2p

This command displays statistical information for protocol analyzers.

With this release, the `yahoomail` keyword is added to the p2p list:

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

show active-charging flows type p2p

This command displays the information for the active charging flows.

With this release, the `yahoomail` keyword is added to the p2p list:

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

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

With this release, the **yahoomail** keyword is added to the p2p list:

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

Performance Indicator Changes

P2P Schema

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

The following bulk statistics are added to the P2P schema:

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

show active-charging analyzer statistics name p2p verbose

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

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

- Yahoomail:
  - Total Uplink Bytes
  - Total Downlink Bytes
  - Total Uplink Packets
  - Total Downlink Packets

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

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

- E-Mail-yahoomail:
  - Total Uplink Bytes
  - Total Downlink Bytes
  - Total Uplink Packets
  - Total Downlink Packets

show active-charging sessions summary
With this release, the following fields have been added to the output of this command:

- Current Yahoomail Sessions

**CSCuj44396 - Support outlook application in P2P detection**

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

**Feature Changes**

**Support for Outlook Application Detection**

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

**Command Changes**

`p2p-detection protocol`  
This command enables detection of peer-to-peer (P2P) protocols.  
With this release, the `outlook` keyword is added to this command:

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

`p2p protocol`  
This command enables detection of specific P2P protocols for charging purposes.  
With this release, the Outlook protocol is supported.

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

`clear active-charging analyzer statistics`  
This command enables detection of specific P2P protocols for charging purposes.  
With this release, the Outlook protocol is supported.
clear active-charging analyzer statistics [ name protocol_name ] [ | { grep grep_options | more } ]

show active-charging analyzer statistics name p2p

This command displays statistical information for protocol analyzers.
With this release, the outlook keyword is added to the p2p list:

show active-charging analyzer statistics name p2p application p2p_list

show active-charging flows type p2p

This command displays the information for the active charging flows.
With this release, the outlook keyword is added to the p2p list:

show active-charging flows type p2p application p2p_list

show active-charging sessions summary

This command displays statistics for Active Charging Service (ACS) sessions.
With this release, the outlook keyword is added to the p2p list:

show active-charging sessions summary type p2p application p2p_list

Performance Indicator Changes

P2P Schema

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

The following bulk statistics are added to the P2P schema:

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

show active-charging analyzer statistics name p2p verbose

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

- Outlook:
  - Total Uplink Bytes
- Total Downlink Bytes
- Total Uplink Packets
- Total Downlink Packets

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

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

- E-Mail-outlook:
  - Total Uplink Bytes
  - Total Downlink Bytes
  - Total Uplink Packets
  - Total Downlink Packets

**show active-charging sessions summary**

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

- Current Outlook Sessions

**CSCuj65264 - ADC Support for Badoo**

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

**Feature Changes**

**Support for Badoo Application Detection**

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

**Command Changes**

**p2p-detection protocol**

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

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

```
configure

active-charging service service_name

[ no ] p2p-detection protocol badoo

end
```

**p2p protocol**
This command enables detection of specific P2P protocols for charging purposes. With this release, the Badoo protocol is supported.

```bash
configure

active-charging service service_name

ruledef ruledef_name

[ no ] p2p protocol badoo

end

clear active-charging analyzer statistics

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

```clear active-charging analyzer statistics [ name protocol_name ] [ | { grep grep_options | more } ] ```

show active-charging analyzer statistics name p2p

This command displays statistical information for protocol analyzers. With this release, the `badoo` keyword is added to the p2p list:

```bash
show active-charging analyzer statistics name p2p application p2p_list
show active-charging flows type p2p

This command displays the information for the active charging flows. With this release, the `badoo` keyword is added to the p2p list:

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

show active-charging sessions summary

This command displays statistics for Active Charging Service (ACS) sessions. With this release, the `badoo` keyword is added to the p2p list:

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

Performance Indicator Changes

P2P Schema

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

The following bulk statistics are added to the P2P schema:
• p2p-badoo-group
• p2p-badoo-uplnk-bytes
• p2p-badoo-dwnlk-bytes
• p2p-badoo-uplnk-pkts
• p2p-badoo-dwnlk-pkts
• p2p-badoo-duration

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

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

- Badoo:
  - Total Uplink Bytes
  - Total Downlink Bytes
  - Total Uplink Packets
  - Total Downlink Packets

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

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

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

**show active-charging sessions summary**

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

- Current Badoo Sessions

**CSCuj65272 - ADC Support Vine**

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

**Feature Changes**

**Support for vine Application Detection**

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

**p2p-detection protocol**

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

With this release, the *vine* keyword is added to this command:

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

**p2p protocol**

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

With this release, the Vine protocol is supported.

```plaintext
configure
  active-charging service service_name
    ruledef ruledef_name
      [ no ] p2p protocol vine
    end
```

**clear active-charging analyzer statistics**

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

With this release, the Vine protocol is supported.

```plaintext
clear active-charging analyzer statistics [ name protocol_name ] [ | { grep grep_options | more } ]
```

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

This command displays statistical information for protocol analyzers.

With this release, the *vine* keyword is added to the p2p list:

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

**show active-charging flows type p2p**

This command displays the information for the active charging flows.

With this release, the *vine* keyword is added to the p2p list:

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

This command displays statistics for Active Charging Service (ACS) sessions.
With this release, the **vine** keyword is added to the p2p list:

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

**Performance Indicator Changes**

**P2P Schema**

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

The following bulk statistics are added to the P2P schema:

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

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

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

- **Vine:**
  - Total Uplink Bytes
  - Total Downlink Bytes
  - Total Uplink Packets
  - Total Downlink Packets

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

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

- **Social-nw-generic-vine:**
  - Total Uplink Bytes
  - Total Downlink Bytes
  - Total Uplink Packets
  - Total Downlink Packets

**show active-charging sessions summary**
With this release, the following fields have been added to the output of this command:

- Current Vine Sessions

**CSCuj82539 - Support for foursquare**

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

**Feature Changes**

**Support for Foursquare Application Detection**

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

**Command Changes**

```
p2p-detection protocol
```

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

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

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

```
p2p protocol
```

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

With this release, the Foursquare protocol is supported.

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

```
clear active-charging analyzer statistics
```

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

With this release, the Foursquare protocol is supported.
clear active-charging analyzer statistics [ name protocol_name ] [ | { grep grep_options | more } ]

show active-charging analyzer statistics name p2p

This command displays statistical information for protocol analyzers.
With this release, the foursquare keyword is added to the p2p list:

show active-charging analyzer statistics name p2p application p2p_list

show active-charging flows type p2p

This command displays the information for the active charging flows.
With this release, the foursquare keyword is added to the p2p list:

show active-charging flows type p2p application p2p_list

show active-charging sessions summary

This command displays statistics for Active Charging Service (ACS) sessions.
With this release, the foursquare keyword is added to the p2p list:

show active-charging sessions summary type p2p application p2p_list

Performance Indicator Changes

P2P Schema

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

The following bulk statistics are added to the P2P schema:

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

show active-charging analyzer statistics name p2p verbose

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

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

- Foursquare:
  - Total Uplink Bytes
• Total Downlink Bytes
• Total Uplink Packets
• Total Downlink Packets

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

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

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

**show active-charging sessions summary**

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

• Current Foursquare Sessions
ADC Enhancements for September 30, 2013

ADC Feature Changes as of September 30, 2013

This section provides information on ADC feature changes in release 15.0.

New ADC Features

This section identifies new ADC features available in release 15.0.

New P2P Protocols Detection Support

This release now supports the detection of the following P2P protocols:

- Baidu Movie
- Bitcasa
- Clubbox
- Dropbox
- Flickr
- Heytell
- Hotspot VPN
- Kuro
- Rodi
- Skydrive
- Tumblr
- Voxer
- Vtok
- Youtube

Modified ADC Features

This section identifies ADC features modified in release 15.0.

None for this release.

ADC Command Changes as of September 30, 2013

This section provides information on ADC command changes in release 15.0.
New ADC Commands

This section identifies new ADC commands available in release 15.0.
None for this release.

Modified ADC Commands

This section identifies ADC commands modified in release 15.0.

**p2p-detection protocol**

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

With this release, the following keywords are added to this command:

- baidumovie
- bitcasa
- clubbox
- dropbox
- flickr
- heytell
- hotspot vpn
- kuro
- rodi
- skydrive
- tumblr
- voxer
- vtok
- youtube

```config
active-charging service service_name
[ no ] p2p-detection protocol [ baidumovie | bitcasa | clubbox | dropbox | flickr | heytell | hotspotvpn | kuro | rodi | skydrive | tumblr | voxer | vtok | youtube ]
end
```

**p2p protocol**
This command enables detection of specific P2P protocols for charging purposes. With this release, the following protocols are also supported:

- baidumovie
- bitcasa
- clubbox
- dropbox
- flickr
- heytell
- hotspot vpn
- kuro
- rodi
- skydrive
- tumblr
- voxer
- vtok
- youtube

```
config

active-charging service service_name

ruledef ruledef_name

[ no ] p2p protocol operator protocol

end
```

clear active-charging analyzer statistics

This command supports the clearing of protocol analyzer statistics. With this release, the following keywords are added to the p2p list:

- baidumovie
- bitcasa
- clubbox
- dropbox
- flickr
- heytell
- hotspot vpn
- kuro
- rodi
show active-charging analyzer statistics name p2p

This command displays statistical information for protocol analyzers.

With this release, the following keywords are added to the p2p list:

- baidumovie
- bitcasa
- clubbox
- dropbox
- flickr
- heytell
- hotspotvpn
- kuro
- rodi
- skydrive
- tumblr
- voxer
- vtok
- youtube

show active-charging flows type p2p

This command displays the information for the active charging flows.

With this release, the following keywords are added to the p2p list:

- baidumovie
- bitcasa
- clubbox
- dropbox
- flickr
show active-charging analyzer flows type p2p application  p2p_list

show active-charging sessions summary

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

With this release, the following keywords are added to the p2p list:

- baidumovie
- bitcasa
- clubbox
- dropbox
- flickr
- heytell
- hotspotvpn
- kuro
- rodi
- skydrive
- tumblr
- voxer
- vtok
- vtok audio
- vtok unclassified
- vtok video
- youtube
show active-charging sessions summary type p2p application p2p_type

Deprecated ADC Commands

This section identifies deprecated ADC commands that are no longer supported in release 15.0.
None for this release.

ADC Performance Indicator Changes as of September 30, 2013

This section provides information on ADC performance indicator changes in release 15.0.

Important: For more information regarding bulk statistics and output fields and counters in this section, refer to the Statistics and Counters Reference for this release.

New ADC Bulk Statistics

This section identifies new ADC bulk statistics available in release 15.0.
New ADC bulk statistics are available in the P2P schema for new protocols/applications as part of the plugin. If detection of a specific P2P protocol is enabled, bulk statistics for that protocol will be automatically generated using the Dynamic Software Upgrade plugin installed on the chassis. In the case of protocols that support sub-classification, the bulk statistics will be generated for each of the supported sub-classifications per protocol and also the corresponding cumulative count.
For a list of new protocols supported in this release, see New P2P Protocols Detection Support.

Modified ADC Bulk Statistics

This section identifies ADC bulk statistics modified in release 15.0.
None for this release.

Deprecated ADC Bulk Statistics

This section identifies deprecated ADC bulk statistics that are no longer supported in release 15.0.
None for this release.

New ADC Output Fields and Counters

This section identifies new ADC show command output fields and counters available in release 15.0.

show active-charging analyzer statistics name p2p verbose

This command displays Active Charging protocol analyzer statistics for the P2P protocol analyzer.
With this release, the following fields have been added to the output of this command to display the uplink bytes, downlink bytes, uplink packets, and downlink packets for the following protocols:

- baidumovie
• bitcasa
• clubbox
• dropbox
• flickr
• heytell
• hotspotvpn
• kuro
• rodi
• skydrive
• tumblr
• voxer
• vtok audio
• vtok unclassified
• vtok video
• youtube

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

With this release, the following fields have been added to the output of this command to display the uplink bytes, downlink bytes, uplink packets, and downlink packets for the following protocols:

• Communicator-vtok
• Communicator-heytell
• Communicator-voxer
• Cloud-skydrive
• Cloud-dropbox
• Cloud-bitcasa
• Cloud-clubbox
• Internet-privacy-hotspotvpn
• Filesharing-flickr
• P2P-filesharing-rodi
• Social-nw-generic-tumblr
• Streaming-kuro
• Streaming-youtube
• Streaming-baidumovie

**show active-charging sessions summary**
With this release, the following fields have been added to the output of this command to display the total number of current sessions for the following protocols:

- baidumovie
- bitcasa
- clubbox
- dropbox
- flickr
- heytell
- hotspotvpn
- kuro
- rodi
- skydrive
- tumblr
- voxer
- vtok
- youtube

Modified ADC Output Fields and Counters

This section identifies modified ADC show command output fields and counters available in release 15.0.
None for this release.

Deprecated ADC Output Fields and Counters

This section identifies deprecated ADC output fields and counters that are no longer supported in release 15.0.
None for this release.
Chapter 3
ECS Changes in Release 15.0

This chapter identifies features and functionality added to, modified for, or deprecated from 15.0 ECS software releases.

**Important:** All functionality from Limited Availability Release StarOS Version 14.1 has been included in General Availability Release StarOS Version 15.0. The *Cisco ASR 5x00 Release Change Reference, Version 14.1*, details new feature descriptions and configuration, performance, and security changes for the 14.1 release.
ECS Enhancements for February 27, 2015

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.

**CSCus74979 - lower-ip-precedence not working when data packet exceeds CIR**

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

**Feature Changes**

**Policing based on committed-data-rate for Non-GBR Bearer**

**Previous Behavior:** The policing based on committed-data-rate was not effected for non-GBR bearers even if it is configured in charging-action configuration mode.

**New Behavior:** Now, the committed-data-rate policing can be implemented for both GBR bearers and non-GBR bearers.

**Customer Impact:** If the customer is not interested in implementing the committed-data-rate policing for non-GBR bearers, then the *committed-data-rate* keyword should not configured with the *flow limit-for-bandwidth* command in charging-action configuration mode.
ECS Enhancements for October 31, 2014

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.

**CSCuo32161 - ASR5K: Need enhanced counters for QGR monitoring**

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

**Feature Changes**

**New Counters for QGR Monitoring**

The following new counters have been added to the existing counters to differentiate the different types of QGRs:

- Total Sessions with Charging-Updates Active Volume Monitoring: 0
- Total Sessions with Charging-Updates Active Bandwidth Limit: 0

**Performance Indicator Changes**

**QGR Schema**

The following new counters have been added to the existing counters to differentiate the different types of QGRs:

- Total Sessions with Charging-Updates Active Volume Monitoring: 0
- Total Sessions with Charging-Updates Active Bandwidth Limit: 0

**show active-charging subsystem all**

The output of the command `show active-charging subsystem all` would display the following counters:

- Total Charging-Updates Received: 0
- Total Charging-Updates Active: 0
- Total Sessions with Charging-Updates Received: 0
- Total Sessions with Charging-Updates Active: 0
- Total Sessions with Charging-Updates Enforced: 0
- Total Sessions with Charging-Updates Active Volume Monitoring: 0
• Total Sessions with Charging-Updates Active Bandwidth Limit: 0

**CSCup67356 - Rule failure counters not incremented**

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

**Feature Changes**

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

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

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

**Performance Indicator Changes**

*show active-charging service statistics*

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

• No active rule in Rulebase/Subs

---

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

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

**Feature Changes**

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

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

*New Behavior:* Now, when the TCP in-order packets are received, the list is checked for any pending packets. If there are any pending packets in the list, the timer is extended so that packet in list can get configured time for reordering.
ECS Enhancements for June 6, 2014

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 *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.

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

**Feature Changes**

flow idle timeout and flow limit for UDP

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

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

**Command Changes**

**show active-charging charging-action statistics**

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

**show active-charging sessions full all**

Earlier, in case of `flow limit-for-flow-type` and `over-limit-action terminate-flow` set for udp packets in charging-action, each dropped `udp packet` was being counted as `ITC Terminated Flows` in this command. Now, each dropped `udp flow` is counted.
ECS Enhancements for April 15, 2014

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 Enhanced Charging Services 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.

**CSCuj77690 - Session Recovery Improvements for GGSN and PGW**

*Applicable Products:* GGSN, P-GW

**Feature Changes**

**Session Recovery Improvements**

**Previous Behavior:** There were only 10 PCC rules that were recovered per bearer in the event of a session manager crash.

**New Behavior:** In this release, this limit has been increased to 24. That is, up to 24 PCC rules can be recovered post ICSR.

With the increase in the limit of PCC rules that can be recovered, the rules are not lost and hence the charging applied to the end users are not impacted.

**CSCul61892 - Ran b/w optimization performed for flow-status other than DISABLED**

*Applicable Products:* P-GW

**Feature Changes**

**RAN Bandwidth Optimization for Uni-directional Flows**

**Previous Behavior:** The rules with flow-status = ENABLE_UPLINK and ENABLE_DOWNLINK were treated similar to the rules with flow-status = DISABLED when the CLI command *ran bandwidth optimize* was configured under rulebase configuration mode. This resulted in allocating lesser bandwidth to the subscriber call.

**New Behavior:** Rules with flow-status = ENABLE_UPLINK and ENABLE_DOWNLINK are now treated similar to the rules with flow-status = ENABLED, thus resulting in sufficient RAN bandwidth allocation for the bearer.

**Customer Impact:** Subscriber calls with bearers containing rules with uni-directional flows will now see sufficient RAN bandwidth allocated for them.
CSCum91142 - PGW rejecting the rule modified by PCRF with QOS_Validation failure

Applicable Products: P-GW

Feature Changes

Previous Rule Processing

Previous Behavior: P-GW was rejecting rules due to QoS Validation failure, although nothing was incorrect about the rule installed. The rule was still being retained although the rule was rejected and reported. This caused failures and session manager crashes.

New Behavior: P-GW now buffers and processes the rule once it receives response for the previous rule request.

Customer Impact: Rule rejection will not be seen in case the previous rule operation is pending access side updates.

CSCun25302 - Rule failure handling: simultaneous change of eval prec & rule content

Applicable Products: P-GW

Feature Changes

Rule Failure Handling

Previous Behavior: In a scenario where two dynamic rules (R1 and R2) were installed on one bearer and when a RAR containing modifications to both the rules was received, the content for rule R1 was modified causing a change in the evaluation precedence value of R2. When the modification of R2 (as received in RAR) was processed, PCEF used to send rule failure report to PCRF. However, the rule R2 was not removed from the bearer.

New Behavior: With this enhancement, in this scenario, the dynamic rule R2 will be removed from the bearer.
ECS Enhancements for March 31, 2014

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 Enhanced Charging Services 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.

### CSCuj77690 - Session Recovery Improvements for GGSN and PGW

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

**Feature Changes**

**Session Recovery Improvements**

**Previous Behavior:** There were only 10 PCC rules that were recovered per bearer in the event of a session manager crash.

**New Behavior:** In this release, this limit has been increased to 24. That is, up to 24 PCC rules can be recovered post ICSR.

With the increase in the limit of PCC rules that can be recovered, the rules are not lost and hence the charging applied to the end users are not impacted.

### CSCul61892 - Ran b/w optimization performed for flow-status other than DISABLED

**Applicable Products:** P-GW

**Feature Changes**

**RAN Bandwidth Optimization for Uni-directional Flows**

**Previous Behavior:** The rules with flow-status = ENABLE_UPLINK and ENABLE_DOWNLINK were treated similar to the rules with flow-status = DISABLED when the CLI command `ran bandwidth optimize` was configured under rulebase configuration mode. This resulted in allocating lesser bandwidth to the subscriber call.

**New Behavior:** Rules with flow-status = ENABLE_UPLINK and ENABLE_DOWNLINK are now treated similar to the rules with flow-status = ENABLED, thus resulting in sufficient RAN bandwidth allocation for the bearer.

**Customer Impact:** Subscriber calls with bearers containing rules with uni-directional flows will now see sufficient RAN bandwidth allocated for them.
CSCum91142 - PGW rejecting the rule modified by PCRF with QOS_Validation failure

**Applicable Products:** P-GW

**Feature Changes**

**Previous Rule Processing**

*Previous Behavior:* P-GW was rejecting rules due to QoS Validation failure, although nothing was incorrect about the rule installed. The rule was still being retained although the rule was rejected and reported. This caused failures and session manager crashes.

*New Behavior:* P-GW now buffers and processes the rule once it receives response for the previous rule request.

*Customer Impact:* Rule rejection will not be seen in case the previous rule operation is pending access side updates.

CSCun25302 - Rule failure handling: simultaneous change of eval prec & rule content

**Applicable Products:** P-GW

**Feature Changes**

**Rule Failure Handling**

*Previous Behavior:* In a scenario where two dynamic rules (R1 and R2) were installed on one bearer and when a RAR containing modifications to both the rules was received, the content for rule R1 was modified causing a change in the evaluation precedence value of R2. When the modification of R2 (as received in RAR) was processed, PCEF used to send rule failure report to PCRF. However, the rule R2 was not removed from the bearer.

*New Behavior:* With this enhancement, in this scenario, the dynamic rule R2 will be removed from the bearer.
ECS Enhancements for February 17, 2014

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 *Enhanced Charging Services 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.

CSCul09884, CSCuf90188 - ECSV2 Volume Usage support post ICSR switchover

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

**Feature Changes**

**ICSR Support for VoRoGx**

**Previous Behavior:** After the ICSR switchover, any existing session for which the PCRF has enabled volume reporting used to continue indefinitely until the session is terminated or until CCR-U is sent for a given trigger, without having the volume counted via Gx.

To summarize, after an ICSR switchover, volume reporting over Gx is no longer done for existing sessions. Also, volume usage is not synced to standby chassis.

**New Behavior:** Volume threshold and Volume usage are synced to standby chassis to support volume reporting over Gx for existing sessions post switchover.

**Customer Impact:** Without this support it cannot cause a subscriber to use higher speeds than what he is supposed to get, if volume reporting is for example used to enforce fair usage; the operator may already consider this a revenue loss. It will also severely impact roaming subscribers who are supposed to get a notification and be blocked/redirected once the limits set by the EU roaming regulation are reached. If a session continues now without being blocked, the operator is not allowed to charge for data beyond the limit and will have a significant and real revenue loss (roaming partner may still charge for the data used on their SGSNs).
ECS Enhancements for January 31, 2014

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 *Enhanced Charging Services 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.

**CSCul09884, CSCuf90188 - ECSV2 Volume Usage support post ICSR switchover**

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

**Feature Changes**

**ICSR Support for VoRoGx**

**Previous Behavior:** After the ICSR switchover, any existing session for which the PCRF has enabled volume reporting used to continue indefinitely until the session is terminated or until CCR-U is sent for a given trigger, without having the volume counted via Gx.

To summarize, after an ICSR switchover, volume reporting over Gx is no longer done for existing sessions. Also, volume usage is not synced to standby chassis.

**New Behavior:** Volume threshold and Volume usage are synced to standby chassis to support volume reporting over Gx for existing sessions post switchover.

**Customer Impact:** Without this support it cannot cause a subscriber to use higher speeds than what he is supposed to get, if volume reporting is for example used to enforce fair usage; the operator may already consider this a revenue loss. It will also severely impact roaming subscribers who are supposed to get a notification and be blocked/redirected once the limits set by the EU roaming regulation are reached. If a session continues now without being blocked, the operator is not allowed to charge for data beyond the limit and will have a significant and real revenue loss (roaming partner may still charge for the data used on their SGSNs).
ECS Enhancements for November 30, 2013

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 Enhanced Charging Services 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.

### CSCub54839 - Full URL in EDR records

**Applicable Products:** HA, PDSN

**Feature Changes**

**Configurable Length for User-Agent and HTPP URL Fields in EDRs**

**Previous Behavior:** The EDR rule-variable for HTPP URL and User-Agent supported the field size of 127 characters. Any URL/User-Agent greater than 127 was truncated and then written to EDR record.

**New Behavior:** The length of HTPP URL and User-Agent fields in generated EDR is made configurable and can be up to a maximum of 255 characters.

For more information, see the ASR 5x00 Command Line Interface Reference.

### CSCuc32951 - EDRs to support User-Agent field greater than 128 bytes

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

**Feature Changes**

**Increased Field Size for HTTP User-Agent and URL in EDRs**

**Previous Behavior:** The maximum field size allowed in the configuration of EDR rule-variable for http url and user-agent was 127. Any URL/User-Agent greater than 127 was truncated and then written to EDR. There were no limits checks placed by HTTP protocol for the length of these fields.

**New Behavior:** An optional filter “length” is supported for HTTP URL and User-Agent which when added will allow the user to configure length from 1 to 255.

**Command Changes**

```
rule-variable
```
An optional filter “length” is supported for HTTP URL and User-Agent rule variables which when added will allow the user to configure the length from 1 to 255.

```
configure
  require active charging
  active-charging service service_name
    edr-format format_name
    rule-variable http url length size priority priority
    rule-variable http user-agent size priority priority
  end
```

**CSCui00558 - Lte call gets terminated when default-eps-bearer-Qos modified in CCA-U**

Applicable Products: P-GW

**Feature Changes**

**Call Handling for Rules Moving to Same QCI as Default Bearer**

**Previous Behavior:** Call gets terminated if default bearer has only dynamic rule on it (no predefined or static rule) and if any one of the following conditions are met:

- It is moved to a new QCI along with a dynamic rule that was already present on default bearer.
- It is moved to a new QCI along with a dynamic rule that was not present on any of the bearers of the call.
- It is moved to a new QCI along with a dynamic rule that was already present on a dedicated bearer.

**New Behavior:** Call remains up in the following two cases after default bearer QCI change.

- It is moved to a new QCI along with a dynamic rule that was already present on default bearer.
- It is moved to a new QCI along with a dynamic rule that was not present on any of the bearers of the call.

Call gets deleted when the bearer is moved to a new QCI along with a dynamic rule that was already present on a dedicated bearer.

**Customer Impact:** A call that had default bearer with only dynamic rule, that is no static or predefined rule, can get terminated if it is moved to a different QCI along with dynamic rules that were already present on any of the dedicated bearers.

**CSCug37786 - Optimized Calculation of GBR MBR based on disabled flows**

Applicable Products: P-GW
Feature Changes

RAN Bandwidth Optimization

When the rule is installed and active, P-GW uses the GBR/MBR assigned in the rule for calculating the GBR / MBR values towards the bearers created. When more than one rule is installed, P-GW adds the GBR / MBR values from all the active and installed rules even if the flow of a certain rule is marked as disabled. This current behavior is in accordance with 3GPP TS standard specification 29.212, and this might result in RAN bandwidth wastage. To avoid this wastage, some optimization is done while calculating MBR and GBR for GBR bearer.

This optimization feature provides the ability to configure a list of APNs, for which the optimized calculation of MBR, GBR can be enabled. By default, this optimized calculation should be enabled only for the IMS APN.

This feature further helps optimize the logic of aggregating MBR and GBR values, based on “Flow-Status” AVP value received in the rule definition through RAR.

Command Changes

`ran bandwidth optimize`

This command is used to enable optimized calculation of [MBR, GBR] when a subscriber (voice) call is put on hold in case of VoLTE.

```
configure
require active-charging
active-charging service service_name
rulebase rulebase_name
[ default | no ] ran bandwidth optimize
end
```

During session setup, when a CCA-I is received, and if `ran bandwidth optimize` is configured for the associated rulebase, the system will aggregate [MBR, GBR] values of only the rules which have flow-status="ENABLED". This information will subsequently be sent to UE.

By default, this CLI will be disabled. Any change in this configuration will not affect existing calls on the system. Optimized bandwidth calculation will be done only for the new calls established after enabling this CLI command.

Performance Indicator Changes

`show active-charging rulebase name`

The following field has been added to the output of this command to indicate if this optimization feature is enabled or disabled.

- Ran Bandwidth Optimization
ECS Enhancements for September 30, 2013

ECS Feature Changes as of September 30, 2013

This section provides information on ECS feature changes in release 15.0.

Important: For more information regarding features in this section, refer to the Enhanced Charging Services Administration Guide for this release.

New ECS Features

This section identifies new ECS features available in release 15.0.

ECS Flow Information to MINE Server

With this release, the ECS flow information and NBR information for a GGSN/PGW subscriber can be sent to the MINE server over the IPNE service client whenever applicable. The MINE server can use the information to trigger policy decisions after analysis and aggregation. The information is forwarded to the MINE server in XMPP format with selector tags defined for ECS and NBR in two modes: Query-Response and Subscribe-Notify.

- Query-Response: In this mode, the MINE server requests the IPNE client for ECS flow and/or NBR information by providing the MSISDN and/or APN Name of a subscriber. IPNE server identifies the subscriber session and requests ECS and NBR modules to collect the required information. IPNE then encodes the information in XMPP format and sends it as response message to the MINE server.

- Subscribe-Notify: In this mode, the MINE server subscribes for ECS flow and/or NBR information for a specific subscriber. Whenever flow creation, updating, and deletion, or NBR allocation/deallocation occurs, the IPNE client is informed. IPNE then sends a notification indicating the change to the MINE server.

Dedicated Trigger for Tethering Detection

This feature simplifies the detection of tethering flow, reduces the number of Gx exchanges, and the configuration impact for IMSA, session manager, and ECS. When tethering is detected for a GGSN or P-GW subscriber, ECS initiates a trigger to PCRF over the Gx interface. When tethering is detected for the first time for a subscriber, ECS sends a message to IMSA to inform of the event. Based on the CLI configuration or trigger set by the PCRF, IMSA forwards the event to the PCRF entity on the network.

DSCP Detection Capability in ECS

This feature enables you to write rules to detect incoming packets belonging to a particular traffic class from DSCP value in the IP ToS header field. Upon detection of traffic class of a packet, each packet can be classified and treated appropriately, and any available charging actions can be applied to the packet on rule matching.

Fastpath Feature

With this release, the Fastpath feature is introduced to reduce the overall system performance impact as a large amount of data packet is consumed through the ECS data path. The Fastpath feature introduces an alternate ECS data path
(Fastpath) with limited supported features. By limiting the supported features, Fastpath eliminates the overhead of packets being subjected to the large number of feature-based conditional checks in ECS.

Fastpath does not replace the existing data path, and works in parallel with the existing ECS data path. The Fastpath feature is part of the Transactional Rule Matching (TRM) feature and requires TRM to be enabled.

For information on ECS features supported by fastpath, refer the Enhanced Charging Services Administration Guide.

Handling/Prioritizing from multiple flow actions for same packet

Flow Actions-related Changes

In this release, the following flow action changes are introduced:

- Multiple flow actions from more than one charging action can be taken on a single packet.
- The flow actions Flow-Kill, Redirection and content-Insertion will interwork with Next Hop and VLAN ID configurations.
- Flow actions are divided into the following broad categories:
  - Buffer
  - Session kill
  - Injections actions
  - Modification actions
  - Common actions
- If a flow action from a particular category cannot be taken on the packet under consideration, then the next flow action from the same category (if set during rule matching) would be considered for application.
- Only one Injection action would be taken on the packet and it would interwork with any or all of the common actions.
- All modification actions will interwork with each other as well as with Common actions.
- Post-processing—Charging hierarchy no longer exists as far as the flow actions are concerned except in those cases concerning the post-processing actions set from the OCS and that in the limit-reached quota state.
- All flow actions can now fall in any of the category (Charging/ Post-processing). That is, no barrier exists in configuring a particular flow action as a charging or post-processing action.
- The charging action/sub session level statistics will get incremented only if the action is taken.
- The injection actions taken on WAP packets will also support the Next Hop and VLAN ID configurations for injected packets.
- The ICAP connection failure actions will not get any special prioritization. They obey the prioritization rules which are laid down.
- In case when the same flow action is configured inside a normal charging action as well as inside the post-processing charging action, the post-processing flow action will take priority.

Post-processing Rule Matching-related Changes

The following post-processing rule matching changes are introduced:

- Post-processing rule matching occurs when post-processing rules are configured and/or the FUI rules are enabled. Post-processing rule matching is ignored only if the packet is buffered by DCCA or ACF.
DCCA-related Changes
The following DCCA changes are introduced:

- After DCCA gets the quota for any packet that it has buffered, the packet will go for post-processing rule matching and the subsequent prioritization. In no case, the post processing rule matching and the corresponding prioritization would be skipped after DCCA gets the renewed quota for the buffered packet.
- For Quota state equal to Limit reached and post processing rule match is successful, any action specified by the post-processing rule match is taken. Else, the action is discarded.
- DCCA specified actions will always have the highest priority over normal charging as well as the post-processing actions.
- For the bytes/packets dropped at the post-processing stage, a counter is incremented at the sub-session level. This counter would denote the packets and bytes dropped at the post-processing level which have been possibly charged by OCS.

ACF-related Changes
The following ACF changes are introduced:

- When a packet gets buffered with ICAP, the disposition action BUFFER is set and the packet does not go for any post-processing rule matching or/and flow action application till ACF does not forward the packet.
- For any of the ICAP injection actions like DENY or Content-Insert or Redirect, the injected packets goes to the readdressed destinations if readdressing flow action has already been taken on the flow.

Idle Timeout-related Changes
The following ACF changes are introduced:

- Idle timeout, if configured inside a post-processing charging action (linked to a matched post-processing rule) always gets a higher priority over the idle timeout configured inside a normal charging action (linked to a matched charging rule.)
- The idle timeout, if configured inside a post-processing charging action, would get applied if the corresponding post-processing rule match occurs.

PCO for UE Notification Updates
With this release, Protocol Configuration Options (PCO) updating is possible using the Gy interface. This value is configurable in the charging action for the corresponding Filter-Id. This enables the P-GW to use PCO to provide additional information to the UE device and display corresponding messages to the user or notify the network status to the device to avoid the device from sending false data to the network. This is useful during user self-activation, out of credit, and time constraint usage control scenarios.

This release introduces the following PCO over UE functionalities:

- P-GW now allows configuration of PCO action value in the post-processing dynamic rules.
- P-GW now includes the PCO information for session termination.
- Multiple Filter IDs from the OCS will now be supported by P-GW using the PCO in the last enabled Filter ID.
- PCO can now be tied with the Filter ID received.
- The Filter-ID sent for deactivation for the Gy interface would be the same as the Filter-ID sent for activation for the PCO update. In the case where a different Filter-ID is requested for deactivation, the Filter-ID is considered as a request for PCO updating to value 0 and a request is sent to the Session Manager accordingly.
- In the case of P-GW to WLAN handover, the last updated PCO is sent to the UE once UE returns to P-GW.
• When the UE is connected to eHRPD, the PCO value of 0 is sent except for Self Activation. When the UE connection returns to P-GW, the last known PCO is sent to the UE and becomes active.

Regular Expression Support for HTTP Referrer Field

With this release, regular expressions can be configured for the HTTP Referrer (HTRF) field in ruledefs.

Transactional Rule Matching Feature

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. This enables ECS to better utilize CPU resources and accommodate additional throughput for the system, thus improving the overall performance.

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

Limitations and Dependencies:

• TRM is supported only on the ASR5500 platform.
• TRM is limited to flows with no protocol routing rules with the exception of HTTP and HTTPS flows. All other flows are not supported and TRM does not have any impact on other flows.
• When TRM is enabled, the following functionalities are affected:
  • Per direction rule matching.
  • TCP state rules for the duration of the TRM transaction.
  • Configuring delay charging when the TRM feature is enabled impacts only packets outside transaction boundaries. All packets within the transaction boundary will be applied to the application (i.e. HTTP).
• Once a flow is classified to a ruledef (first packet in flow for UDP, or the first data packet after the 3-way handshake for a TCP flow), TRM will attempt to use that matched rule for the duration of the transaction. This might result in the ruledefs such as those with mid-transaction TCP states or packet direction to be ignored for the flow.
• Configuring TRM and P2P in the same rulebase is not supported. Any attempt in configuring TRM and P2P in the same rulebase will result in an error message and configuration failure.

Modified ECS Features

This section identifies ECS features modified in release 15.0.

ECS Performance Optimization for IP Fragmentation

Previous Behavior: Rule matching and identification of bearer occurs only after all the fragments of an IP packet are reassembled. The IP fragment-related data structures are maintained at a sub session level. After reassembly, if the packet belongs to another bearer, all the fragment related information is moved to the correct bearer. This leads to performance impact and possibilities for issues.

New Behavior: With this release, handling of IP fragment related structure has been changed to improve performance and reduce the occurrence of issues.

ECS Ruledef Information Enhancements to Monitor Protocol and Monitor Subscriber
In earlier releases, the functionality of the `monitor protocol` and `monitor subscriber` commands was limited to displaying only the packet information that goes in and comes out of ECS. With this release, these commands support tracing rule matches per packet for single subscribers. This information can be used for debugging, and enables better utilization of system resources.

For normal static, predefined or dynamic rule matching, if there is no delay charging or if the data is not segmented (HTTP segmented GET request), rule match is logged as soon as the rule match condition is met.

For HTTP packets with partial header, the packet which contains the end of the header will be rule matched and the previous packet with the partial header will be matched to the rule that the last packet has been matched to.

**ECSv2-DCCA Enhancements**

**DCCA Charging of HTTP/WAP Concatenated Packet Buffered at DCCA**

**Previous Behavior:** In earlier releases, when an HTTP packet (or WAP) containing multiple requests/responses gets buffered at DCCA waiting for a response from OCS regarding the quota for any of these requests, the requests that follow are not forwarded for rule matching. Hence the correct charging action is not applied for these. Additionally, when the quota response is received, the request that caused buffering gets charged against the correct Content ID, while requests that follow are charged against the Content ID of the next packet.

**New Behavior:** With this release, correct rule matching and charging action is taken for subsequent request/response (WAP / HTTP) in a concatenated packet, when the packet is buffered at DCCA waiting for quota response for the earlier request/response. Additionally, all the requests/responses in the buffered concatenated packet are charged for the correct byte count against the correct Content IDs.

**Flow Action Prioritization of Concatenated Packet**

**Previous Behavior:** In earlier releases, when a concatenated (HTTP/WAP) packet is being processed, rule matching and charging occurs per request/response, and the corresponding flow-action is taken on the whole packet per request/response immediately.

**New Behavior:** With this release, when a concatenated (HTTP/WAP) packet is processed, rule matching and charging occurs per request/response. However, the corresponding flow-action will not be taken immediately. The flow action prioritization module marks the flow actions of all the requests/responses and when the whole packet gets processed, a prioritized flow action (from the ones that are marked) will be taken on the whole packet.

**Enhancements to Static, Dynamic, and Predef Rules**

The static rule, dynamic rule, and charging action (billing policy) mapped to a packet after a rule match can deactivate when the packet is buffered at one of the deferal paths, waiting for a service response (For example DCCA buffering, ICAP buffering etc). After the response is received and the packet gets post processed, it has the dangling references to deactivated objects. Also if they are dereferenced somewhere, it results in a segmentation fault.

**Dynamic Rule (Defined and Pushed by PCRF over Gx)**

**Previous Behavior:** Matched dynamic-rule/billing policy of the DCCA buffered packet was not validated after a quota response is received. In cases where the dynamic rule gets deleted before the quota response is received, the packet was being sent to charging and post processing with reference to a non-existent dynamic rule/billing policy. This might lead to a system crash.

**New Behavior:** On dynamic rule deletion, the references to the dynamic rule/ billing policy mapped to the packet after rule match are cleared for the DCCA buffered packets. After the quota response is received, such packets will not be sent for charging or post processing, and will be dropped.
Static Rule and Predef Rules (Activated over Gx)

**Previous Behavior:** The matched rule/ billing policy for DCCA buffered packets was validated after getting the quota response. On receiving the quota response, the packet with the matched rule/ billing policy which no longer exist was not sent for charging, however it was being sent to post processing and then sent out (without charging).

**New Behavior:** After receiving the quota response for the buffered packet, if a mapped static rule/ billing policy no longer exist, it will not be sent for charging or post processing, and will be dropped.

Maximum Number of group-of-ruledefs Increased

A group-of-ruledef is a logical collection of multiple ruledefs that have a similar charging action.

**Previous Behavior:** In earlier releases, a maximum of 64 group-of-ruledefs can be configured.

**New Behavior:** With this release, a maximum of 128 group-of-ruledefs can be configured.

Maximum Number of Rule Lines in a Ruledef Increased

A ruledef is a collection of rule-lines configured on the action-priority line of a rulebase.

**Previous Behavior:** In earlier releases, a maximum of 10 rule-lines can be configured per ruledef.

**New Behavior:** With this release, a maximum of 32 rule-lines can be configured per charging, routing, and post-processing ruledef.

Optimization of Host-pool and Port-Range based rule-lines

Host pools are used to specify a complex set of IP addresses that include unique IP addresses, IP addresses with masks, or IP address ranges, and are used for rule matching.

**Previous Behavior:** In earlier releases, the implementation of host-pool based rule-lines is slow with significant performance impact.

**New Behavior:** With this release, the implementation of host-pool based rule-lines is optimized using an optimization engine that stores the host-pool based rule-lines and matches them optimally, resulting in a better performance. The `debug acsmgr show rule-optimization` command now shows host-pools as optimized.

Optimization of Port-range based rule-lines

**Previous Behavior:** In earlier releases, the implementation of port-range based rule-lines is slow with significant performance impact.

**New Behavior:** With this release, the implementation of port based rule-lines is optimized using an optimization engine to optimize rule-lines that configure TCP or UDP ports using operators range and port-map, resulting in a better performance. The `debug acsmgr show rule-optimization` command now shows port-maps as optimized.

Parse OS-Signature with Tethering Detection Disabled

This release enables os-signatures to be collected from TCP SYN even when tethering detection is disabled from the rulebase. This is useful to collect os-signatures which can be used to build an OS database for the tethering detection feature.

**Previous Behavior:** The os-signature was parsed only when tethering detection is enabled in rulebase.

**New Behavior:** Even when tethering detection is disabled, os-signature will be parsed if an EDR/UDR with an os-signature variable is present in a rulebase, or charging-action in the rulebase.

Performance Optimization for Deep Packet Inspection
**Previous Behavior:** In earlier releases, the HTTP analyzer parses all the fields in the HTTP header even when any rule matching fields or ECS feature does not use the value parsed from the HTTP header, thus impacting the Deep Packet Inspection (DPI) performance.

**New Behavior:** With this release, selective parsing of the HTTP header fields is introduced based on the configured features and rule matching fields using the HTTP header fields. The HTTP header field is parsed only during the following conditions:

- A rulebase configuration refers to a ruledef that requires an HTTP header field for rule matching.
- A charging action that uses an HTTP header field for flow action that uses an HTTP header field information.
- An ECS feature defined at a rulebase level requires an HTTP header field information.

**ECS Command Changes as of September 30, 2013**

This section provides information on ECS command changes in release 15.0.

**Important:** For more information regarding commands in this section, refer to the Command Line Interface Reference for this release.

**New ECS Commands**

This section identifies new ECS commands available in release 15.0.

**http referer**

This command allows you to define rule expressions to match the value in the HTTP Referer request-header field. With this release, the `regex` keyword is added to match the HTRF fields using regular expressions.

```
config

active-charging service service_name

ruledef ruledef_name

http referer [ case-sensitive ] regex string

end
```

**ip dscp**

This command enables you to configure a charging ruledef with the DSCP value and match it with the DSCP value in the incoming IP packets.

```
config

active-charging service service_name

ruledef ruledef_name

[ no ] ip dscp { != | = } { IPv4_ToS | IPv6_TC_value } [ mask mask_value ]
```
transactional-rule-matching

To enable the transactional rule matching feature, use the following configuration:

```
config

active-charging service service_name

rulebase rulebase_name

[ no | default ] transactional_rule_matching

end
```

Notes:
- Use the `no transactional-rule-matching` command or `default transactional-rule-matching` command to disable transactional rule matching.
- Transactional rule matching is disabled by default.

Modified ECS Commands

This section identifies ECS commands modified in release 15.0.

idle-timeout

This command allows you to configure the maximum duration a flow can remain idle for, after which the system automatically terminates the flow.

With this release, the `half-open` keyword is added to the `idle-timeout tcp` command to set idle time out period for half open TCP connections.

```
active-charging service service_name

idle-timeout tcp half-open idle_timeout

[ default | no ] idle-timeout tcp half-open

end
```


Deprecated ECS Commands

This section identifies deprecated ECS commands that are no longer supported in release 15.0.

None for this release.

ECS Performance Indicator Changes as of September 30, 2013

This section provides information on ECS performance indicator changes in release 15.0.
Important: For more information regarding bulk statistics and output fields and counters in this section, refer to the Statistics and Counters Reference for this release.

New ECS Bulk Statistics

This section identifies new ECS bulk statistics available in release 15.0.

New in the ECS Schema

The following statistics are included in the ECS Schema to calculate the current number of Gx dynamic rules per session in P-GW:

- ecs-cur-gxdynrules-per-session

The following statistics are included in the ECS Schema in support of the Transactional Rule Matching feature:

- trm-rule-match-bypassed
- trm-rulematch-bypass-triggered

The following statistics are included in the ECS Schema in support of the Fastpath feature:

- fp-eligible-flows
- fp-packets
- fp-failures

The following statistics are included in the ECS Schema in support of the Tethering Detection feature:

- ecs-td-current-tethered-subscribers
- ecs-td-tethered-uplink-packets
- ecs-td-tethered-downlink-packets

Modified ECS Bulk Statistics

This section identifies ECS bulk statistics modified in release 15.0.

None for this release.

Deprecated ECS Bulk Statistics

This section identifies ECS bulk statistics modified in release 15.0.

None for this Release.

New ECS Output Fields and Counters

This section identifies new ECS show command output fields and counters available in release 15.0.

show active-charging charging-action

The following counter has been introduced for the PCO for UE notification feature:
- PCO

**show active-charging sessions**

The following counter has been introduced in the PCO section of the display for the UE notification feature:
- Value/Interface

**show active-charging flows full**

The following statistic is included in the output of the `show active-charging flows full` command in support of the FastPath feature:
- FP Packets
- FastPath Eligible

The following statistics are introduced in support of the Tethering Detection feature:
- Tethering detection performed
- Tethering detected

**show active-charging rulebase**

The following statistic is included in the output of the `show active-charging rulebase rulebase_name` command in support of the Fastpath feature:
- FastPath Eligible Flows
- FastPath Packets
- FastPath Failures

**show active-charging rulebase name**

The following statistic is included in the output of the `show active-charging rulebase name rulebase_name` command in support of the Transactional Rule Matching feature:
- Transactional-Rule-Matching

The following statistics are introduced in support of the Tethering Detection feature:
- Tethering Detection
- OS-database-used
- UA-database-used

**show active-charging rulebase statistics**

The following statistics are included in the output of the `show active-charging rulebase statistics` command in support of the Transactional Rule Matching feature:
- TRM Statistics
  - Bypassed rule-matching
  - Rule-matching bypass triggered
  - Failed to create dynamic flow element
• Flow cleared, rule not found
• Flow cleared, rule stats not found
• Flow cleared, group not found
• Flow cleared, group rule error
• Flow cleared, rule error
• Flow cleared, rule expired
• Flow cleared, pkts not forwarded
• Flow cleared, pkts buffered
• Flow cleared, SEF event

The following statistics are introduced in support of the Tethering Detection feature:
• Tethering Detection
  • TAC ID lookups
  • TAC ID matches
  • OS signatures lookups
  • OS signatures matches
  • UA signatures lookups
  • UA signatures matches
  • Total flows scanned
  • Tethered flows detected
  • Non-tethered flows detected

**show active-charging ruledef statistics**

The following statistic is included in the output of the `show active-charging ruledef statistics` command in support of the Transactional Rule Matching feature:
• Match-Bypassed

**show active-charging sessions full**

The following statistic is included in the output of the `show active-charging sessions full` command in support of the Transactional Rule Matching feature:
• Match-Bypassed

**show active-charging regex status all**

The following statistic is included in the output of the `show active-charging regex status all` command as part of updates to the regular expression support for http referer
• HTRF

**show active-charging regex statistics ruledef instance**
The following statistic is included in the output of the `show active-charging regex statistics ruledef instance instance_number` command as part of updates to the regular expression support for http referer:

- HTTP REFERER

**show active-charging regex statistics ruledef summary**

The following statistic is included in the output of the `show active-charging regex statistics ruledef summary` command as part of updates to the regular expression support for http referer:

- HTTP REFERER
  - Total Rulelines
  - Matching Skipped Engine Not Ready

**show active-charging sessions full all**

The following statistics are added to the output of the `show active-charging sessions full all` command:

- tethering-detection notification
- tethering-detected notification sent

The following statistics are added to the output of the `show active-charging sessions full all` command to display the post-processing ruledef statistics information to identify the amount of traffic using post-processing ruledefs:

- Post-processing Rulestats
  - Ruledef Name
  - Pkts-Down
  - Bytes-Down
  - Pkts-Up
  - Bytes-Up
  - Hits

**show active-charging subscribers full all**

The following fields and counters are included in the output of the `show active-charging subscribers full all` command in support of the ECS flow information to the MINE server:

- IPNE
- Flow Information
  - Subscriptions
  - Notifications
- NBR Information
  - Subscriptions
  - Notifications

**show active-charging subsystem all**
The following statistic is included in the output of the `show active-charging subsystem all` command in support of the Fastpath feature:

- Total Fastpath flows
- Total Fastpath pkts
- Total Fastpath NAT pkts
- Total Fastpath failures
- Last Fastpath Failure

**show active-charging tethering-detection stats**

The following statistics are added to the output of this command:

- Current tethering-detected indications sent
- Total tethering-detected indications sent

**show active-charging tethering-detection database sessmgr all**

The following fields have been added to the output of the `show active-charging tethering-detection database sessmgr all` command:

- SMgr Instance
- OS Signature Database
  - Source File
  - Database Status
  - Version
  - Number of signatures in DB
  - Last Upgrade Status
- UA Signature Database
  - Source File
  - Database Status
  - Version
  - Number of signatures in DB
  - Last Upgrade Status
- TAC Database
  - Source File
  - Database Status
  - Version
  - Number of entries in DB
  - Last Upgrade Status
show active-charging analyzer statistics name tcp

The following counters have been added to the output of the `show active-charging analyzer statistics name tcp` command to display information about sessions without SYN for TCP:

- Total Non-Syn Flows
- Current Non-Syn Flows

### Modified ECS Output Fields and Counters

This section identifies modified ECS show command output fields and counters available in release 15.0.

**show active-charging subsystem all**

This command displays information of the active charging service subsystem.

The following counters have been changed to display bucket for packets that are sized 1500 and above, as the MTU is normally sized around 1440:

- Data statistics
  - size < 17
  - size 17..64
  - size 64..127
  - size 128..255
  - size 256..511
  - size 512..1023
  - size 1024..1500
  - size 1501..2047
  - size 2048..4095
  - size > 4095

**show active-charging flows summary**

The following counters have been enhanced in the output of the `show active-charging flows summary` command with additional counters in order to provide more information:

In previous releases:

- Total Active Charging Flows
- Uplink Bytes
- Downlink Bytes
- Uplink Pkts
- Downlink Pkts

With this release:

- Current:
- Active Flows
- Idle Flows
- TCP Active flows
- TCP Idle Flows
- UDP Active flows
- UDP Idle Flows
- ICMP Active flows
- ICMP Idle Flows
- ICMPV6 Active flows
- ICMPV6 Idle Flows
- DNS Active flows
- DNS Idle Flows

- Cumulative:
  - Uplink Bytes
  - Downlink Bytes
  - Uplink Pkts
  - Downlink Pkts

**show active-charging ruledef statistics all post-processing**

The output of the `show active-charging ruledef statistics all post-processing` command has been modified to display the output in SSD format.

**Deprecated ECS Output Fields and Counters**

This section identifies deprecated ECS output fields and counters that are no longer supported in release 15.0.

None for this release.
Chapter 4

ePDG Changes in Release 15.0

This chapter identifies features and functionality added to, modified for, or deprecated from 15.0 ePDG software releases.

**Important:** All functionality from Limited Availability Release StarOS Version 14.1 has been included in General Availability Release StarOS Version 15.0. The *Cisco ASR 5x00 Release Change Reference, Version 14.1*, details new feature descriptions and configuration, performance, and security changes for the 14.1 release.
ePDG Enhancements for March 31, 2014

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
- ADC Enhancements
- CF Enhancements
- ECS Enhancements
- Firewall Enhancements
- GTPP Enhancements
- Lawful Intercept Enhancements
- MVG Enhancements
- NAT Enhancements
- SNMP MIB Enhancements
- System & Platform Enhancements

---

**CSCum89534 - ePDG sends LVC traffic over S2b using default bearer not dedicated**

**Feature Changes**

LVC traffic over S2b

**Command Changes**

`ip fragment-chain`
New command `ip fragment-chain { max-ooo-fragment fragments | timeout secs }` is introduced in this release.

```
configure > context context_name > epdg service service_name

    ip fragment-chain { max-ooo-fragment fragments | timeout secs }

    default ip fragment-chain { max-ooo-fragment | timeout }
```
ePDG Enhancements for November 30, 2013

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
- ADC Enhancements
- CF Enhancements
- ECS Enhancements
- Firewall Enhancements
- GTPP Enhancements
- Lawful Intercept Enhancements
- MVG Enhancements
- NAT Enhancements
- SNMP MIB Enhancements
- System & Platform Enhancements

---

CSCuj62118 - [ePDG] - MAC Address extraction based on configured delimiter

**Command Changes**

```bash
username mac-address-delimiter
```

With this release, the `username mac-address-delimiter { NAI-label | colon | colon-or-NAI-label }` keyword has been added to the ePDG Service Configuration Mode commands.

```bash
configure

    context context_name

    epdg-service service_name
```
username mac-address-delimiter { NAI-label | colon | colon-or-NAI-label }
end

CSCui21539 - ePDG and HeNBGW combo

Feature Changes

RFC822 Compliance

**Previous Behavior:** Di contains the NAI in the form "0<IMSI>@ AP_MAC_addr:nai.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org" per 23.003 section 19.3 with the addition of the WiFi access point MAC address. The MAC address of the AP is included in the user name between the ?@? and ?? symbols.

**New Behavior:** Two demarcation characters in an RFC822 format is not allowed. MAC address format is changed to: "0<IMSI>@ AP_MAC_addr.nai.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org" where the MAC address is include between the ?@? and ".nai"

ePDG will extract the string between '@' character and ".nai" string and validate to find the MAC Address. If ePDG will not find the ".nai" after the '@' character in NAI then ePDG will consider, MAC Address of AP is not present in NAI.

CSCui42954 - [ePDG] - MAC Address reporting to support @ AP_MAC_addr.nai NAI format

Command Changes

**show/clear commands**

With this release, the **epdg-service service_name** keyword has been added to the output of the following Exec Mode commands:

- show subscribers active
- show subscriber activity
- show subscribers card-num
- show subscribers connected-time
- show subscribers counters
- show subscribers data-rate
- show subscribers ebi
- show subscribers full
- show subscribers idle-time
show subscribers imsi
show subscriber msid
show subscribers network-type
show subscribers qci
show subscribers rx-data
show subscribers smgr-instance
show subscribers subscription full
show subscribers summary
show subscribers tft
show subscribers tx-data
show subscribers username
show subscribers wfl

clear subscribers active
clear subscribers card-num
clear subscribers connected-time
clear subscribers idle-time
clear subscribers imsi
clear subscribers msid
clear subscribers network-type
clear subscribers rx-data
clear subscribers smgr-instance
clear subscribers tx-data
clear subscribers username
clear subscribers ebi
ePDG Enhancements for September 30, 2013

ePDG Feature Changes as of September 30, 2013

This section provides information on system feature changes in release 15.0.

**Important:** For more information regarding features in this section, refer to the *System Administration Guide* for this release.

New ePDG Features

This section identifies new ePDG features available in release 15.0.

**ICSR**

The ePDG supports ICSR with fault detection and automatic switch over. Subscriber session details for all ePDG interfaces are replicated in STANDBY. In case of a switchover, the new chassis processes all subsequent control and data traffic for the subscriber session.

**ePDG APN-NI: SWu (IDr) interworking with SWm (Service-Selection AVPAPN-NI+OI Support)**

According to 3GPP TS 23.003 section 9.1, section 19.4 and TS 29.303 section 5.1.2, ePDG needs to be enhanced for accepting the APN NI+OI received from UE in GPRS format.

**Previous Behavior:** ePDG only supports APN-NI format being received on Sway interface and further communicate the same over Sum and S2b interface. ePDG does not handles the OI part of APN.

**New Behavior:** ePDG does support APN NI and also APN NI+OI formats of APN being received over Sway interface. ePDG does extracts only APN-NI part and accordingly send the same over Sum interface. Over S2b interface ePDG does sends APN NI+OI and the OI formation is done using the OI received over Sway interface or using the IMSI for default OI creation.

**[ePDG] - S2b on GTP to support IPv4 transport**

The ePDG supports both IPv4 and IPv6 modes for S2B On GTPv2.

The disconnect reason "Transport-mismatch-with-pgw" is reused to disconnect the PMIPv6 call, when IPv4 PGWaddress is received during static/dynamic PGW selection

**Previous Behavior:** Only IPv6 supported for communication over S2b interface towards PGW, GTP.

**New Behavior:** IPv4 along with IPv6 supported for communication over S2b interface towards PGW, GTP.

Modified ePDG Features

This section identifies ePDG features modified in release 15.0.

**PGW re-selection on call attempt failure due to PGW reject**

ePDG selects alternative PGW when first PGW rejects the call.
**ePDG Changes in Release 15.0**

**Previous Behavior**: ePDG does support attempt of call establishment to alternate PGW FQDN when the previous attempt PGW is not responding. In case the PGW has responded rejecting the call ePDG currently clears the call and does not attempt to other PGW.

**New Behavior**: ePDG shall be attempting call establishment to other PGW in case the call is rejected with specific error codes which may be due to resource limitations at PGW which is rejecting the call. This shall help in more successful call establishment rate in network. ePDG needs to try an alternate PGW per the DNS response in case the first PGW has rejected the call with below error causes.:

- EGTP_CAUSE_ALL_DYNAMIC_ADDR_OCCUPIED (0x54)
- EGTP_CAUSE_NO_RESOURCES_AVAILABLE (73)
- EGTP_CAUSE_SERVICE_DENIED (0x59)
- EGTP_CAUSE_PEER_NOT_RESPONDING (100)
- EGTP_CAUSE_SERVICE_NOT_SUPPORTED (0x44)

For all other (besides one mentioned above) GTP call reject cause the behavior shall be clearing the call when rejected by PGW and not attempting on alternate PGWs.

ePDG shall be having the handling for the above mentioned GTPv2 causes in similar manner to PGW not responding. The disconnect reason shall also be same as PGW not reachable.

**ePDG APN-NI: SWu (IDr) interworking with SWm (Service-Selection AVPAPN-NI+OI Support)**

According to 3GPP TS 23.003 section 9.1, section 19.4 and TS 29.303 section 5.1.2, ePDG needs to be enhanced for accepting the APN NI+OI received from UE in GPRS format.

**Previous Behavior**: ePDG only supports APN-NI format being received on SWu interface and further communicate the same over SWm and S2b interface. ePDG does not handles the OI part of APN.

**New Behavior**: ePDG does support APN NI and also APN NI+OI formats of APN being received over SWu interface. ePDG does extracts only APN-NI part and accordingly send the same over SWm interface. Over S2b interface ePDG does sends APN NI+OI and the OI formation is done using the OI received over SWu interface or using the IMSI for default OI creation.

**RFC 5996 Compliance**

Support for processing TEMPORARY_FAILURE and CHILD-SA_NOT_FOUND has been added in accordance to the RFC Specification.

During re key of IKE or CHILDSA, ePDG does not change parameters/algorithms for SA negotiation. Even in case it has multiple transforms configured, it sends only the ones that were selected as part of initial negotiations i.e. IKE-SA-INIT (for IKESA rekey) or IKE-AUTH (for CHILDSA rekey).

UDP encapsulation for inbound packets is supported even for non-NAT'ed sessions.

Certificate exchange is supported using hash-and-url encoding as well. This reduces the size of IKE packet sent by ePDG is ePDG is authenticating using Certificates.

**Modified ePDG Commands**

This section identifies ePDG commands modified in release 15.0.
Staros IKEv2 stack currently complies to RFC 4306. In Release 15.0, Staros IKEv2 is enhanced to comply to newer version of IKEV2 RFC 5996.

```
config

crypto template crypto_map_name ikev2-dynamic ikev2-ikesa policy use-rfc5996-notification
```

**RFC 5996 Support - child sa rekey changes**

According to RFC 5996 on rekeying of a CHILD SA, the traffic selectors and algorithms match the ones negotiated during the setting up of child SA. ePDG is enhanced to not send any new parameters in CREATE_CHILD_SA for a childsa being rekeyed. However ePDG does not enforce any restrictions on the peer for the same. This is done to minimize impact on IOT’s with existing peer vendor products, which may not be complying to RFC 5996.

```
config

crypto template name ikev2-dynamic ikev2-ikesa rekey disallow-param-change
```

**RFC 5996 Support - HTTP_LOOKUP in CERTREQ**

RFC 5996 mandates configurability for sending and receiving HTTP method for hash-and-URL lookup with CERT/CERTREQ payloads. If configured and if peer requests for CERT using encoding type as "Hash and URL of X.509 certificate" and send HTTP_CERT_LOOKUP_SUPPORTED using notify payload in the first IKE_AUTH, ASR shall send the URL in the CERT payload instead of sending the entire certificate in the payload. If not configured and CERTREQ is received with encoding type as "hash and URL for X.509 certificate", ePDG shall respond with entire certificate as it in release 14.1, even if peer had sent HTTP_CERT_LOOKUP_SUPPORTED.

```
config

certificate name cert_name pem_data pem_data private-key pem encrypted data pem_data
cert-enc cert-hash-url url url
```

**ePDG Command Changes as of September 30, 2013**

This section provides information on system-level command changes in release 15.0.

**Important:** For more information regarding commands in this section, refer to the Command Line Interface Reference for this release.

**New ePDG Commands**

This section identifies new ePDG commands available in release 15.0.

```
no allow duplicate-prec-in-tft
```
A new command enables the operator to control how the PGW issues duplicate precedence value in Create Session request (default bearer) and dedicated bearer for LVC/VoLTE, this is seen in a scenario when LVC call hands over to WLAN/ePDG.

```yaml
config
  context context_name
    epdg-service service_name
      no allow duplicate-prec-in-tft
    end
```

**Modified ePDG Commands**

This section identifies system commands modified in release 15.0.
None for this release.

**Deprecated ePDG Commands**

This section identifies system commands that are no longer supported in release 15.0.

**IPv4 address gtpu-service**

Redundant CLI to unbind an IPv4 address in the GTPU service configuration mode is removed.

```yaml
config
  context context_name
    gtpu-service gtpu_service
      no ipv4-address
    end
```

**ePDG Performance Indicator Changes as of September 30, 2013**

This section provides information on system-level performance indicator changes in release 15.0.

**Important:** For more information regarding bulk statistics and output fields and counters in this section, refer to the Statistics and Counters Reference for this release.

**New ePDG Bulk Statistics**

This section identifies new system bulk statistics available in release 15.0.

**New in the ePDG Schema**
New bulkstat **Invalid APN** added to report ePDG rejecting the call on SWu interface due to invalid format of APN. ePDG shall be rejecting the IKE_AUTH_REQUEST message if invalid APN is received and increment this bulkstats before communicating over SWm interface.

**Modified ePDG Bulk Statistics**

This section identifies system bulk statistics modified in release 15.0.

**Modified in the ePDG Schema**

The **Invalid APN** bulkstats is modified to be used for rejecting the invalid format of APN or length validation failure for APN when received on SWu interface. Previously it was used for the mismatch of APN between SWu and SWm interface.

**Deprecated ePDG Bulk Statistics**

This section identifies system bulk statistics that are no longer supported in release 15.0

None for this release.

**New ePDG Output Fields and Counters**

This section identifies new system output fields and counters available in release 15.0.

None for this release.

**Modified ePDG Output Fields and Counters**

This section identifies system output fields and counters modified in release 15.0.

None for this release.

**Deprecated ePDG Output Fields and Counters**

This section identifies system output fields and counters that are no longer supported in release 15.0.

None for this release.
Chapter 5
eWAG Changes in Release 15.0

This chapter identifies features and functionality added to, modified for, or deprecated from 15.0 eWAG software releases.
eWAG Enhancements for January 31, 2014

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

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

CSCuh44969 - eWAG support for multiple primary contexts

**Feature Changes**

**Multiple Primary Context Support**

**Previous Behavior:** In earlier releases, only one PDP was supported for Wi-Fi sessions on R-eWAG.

**New Behavior:** With this release, multiple PDPs are supported on R-eWAG. Multiple calls with the same IMSI number is supported by assigning different NSAPI values for each context. The maximum number of contexts per IMSI can be configured. A new NSAPI value is allocated to the new context until the configured limit is reached. This enables subscribers to access Wi-Fi services from multiple devices at the same time.

For more information on support for multiple primary context, refer to the *Enhanced Wireless Access Gateway Administration Guide*.

**Customer Impact:** Multiple device support is added.

**Command Changes**

`gtp max-contexts-per-imsi`

This command allows you to configure multiple primary contexts having the same IMSI number.

```
configure

context context_name

ipsg-service service_name mode radius-server

  gtp max-contexts-per-imsi max_value min-nsapi min_nsapi_value

default gtp max-contexts-per-imsi

end
```

Notes:
• Use the `gtp max-contexts-per-imsi max_value min-nsapi min_nsapi_value` command to configure the maximum number of contexts per IMSI, and the range of NSAPI values to be assigned to different PDP context.

• Use the `default gtp max-contexts-per-imsi` to configure this command to disable use of multiple primary contexts. Only one PDP context per user is allowed.
eWAG Changes in Release 15.0

This section identifies all of the eWAG enhancements included in this release.

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

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

---

**CSCub53946 - D-eWAG: eWAG to support Local Traffic breakout**

**Feature Changes**

**D-eWAG Local Breakout Feature**

The Local Traffic Breakout feature supports forwarding data that does not require 3G access directly to the Internet. With Local Traffic Breakout support the traffic carried by UE’s will typically fall into one of the following categories:

- WLAN Direct IP Access: This will carry part of the traffic that will go directly over the Internet. The Gn' interface will be bypassed.
- WLAN 3GPP IP Access: This will carry the 3G traffic that will go in the GTPU tunnel towards the MPC (GGSN).
D-eWAG acts as the AAA proxy as well as DHCP-Server to the UE attaching to the WLAN network. While acting as DHCP-Server, DeWAG will create the PDP-Context with GGSN to obtain the IP address to be allocated to the UE through DHCP-Response in the access-side. After the session is created, data is allowed to go through the MPC or directly over the Internet.

**Important:** For Local Traffic Breakout support, D-eWAG requires Dynamic NAT functionality for which ACS and NAT in-line service licenses are required.

### Performance Indicator Changes

**show subscribers full all**

This command displays all available details for active subscribers. The output of this command includes the following new fields:

- Local Breakout input pkts: Indicates the number of packets sent by UE directly to the Internet.
- Local Breakout output pkts: Indicates the number of packets received by UE directly from the Internet.
- Local Breakout input bytes: Indicates the number of bytes sent by UE directly to the Internet.
- Local Breakout output bytes: Indicates the number of bytes received by UE directly from the Internet.

### CSCud96431 - D-eWAG: eWAG support on PSC3 cards

**Feature Changes**

**Support on PSC3 Cards**

With this release, the D-eWAG service in the ASR 5000 can run in PSC3 cards.

### CSCue18931 - D-eWAG: Add Additional Radius AVP support For Local Break Out

**Feature Changes**

**RADIUS AVPs for D-eWAG Local Breakout Feature**

The following RADIUS AVPs have been added in support of the Local Breakout feature:

- SN-LBO-Acct-IN-Pkts: Indicates the number of packets sent by UE directly to the Internet.
- SN-LBO-Acct-Out-Pkts: Indicates the number of packets received by UE directly from the Internet.
- SN-LBO-Acct-IN-Octets: Indicates the number of octets sent by UE directly to the Internet.
- SN-LBO-Acct-Out-Octets: Indicates the number of octets received by UE directly from the Internet.
CSCue63798 - D-eWAG: Support Radius Accounting for Local Breakout

Feature Changes

RADIUS Accounting Support for DeWAG Local Breakout Feature

RADIUS accounting support is now supported for DeWAG Local Breakout feature.
eWAG Feature Changes as of September 30, 2013

This section provides information on eWAG feature changes in release 15.0.

Important: For more information regarding features in this section, refer to the eWAG Administration Guide for this release.

New eWAG Features

This section identifies new eWAG features available in release 15.0.

R-eWAG Support for GGSN-initiated UPC

R-eWAG now supports processing GGSN-initiated UPC requests. GGSN-initiated UPC requests will be accepted only for QoS Update case. In GGSN-initiated UPC request for QoS update, QoS is updated for the R-eWAG session and accept status is sent in UPC response. UPC requests with EUA update, PCO update, APN restriction update, TFT update, and direct tunnel update will be rejected by the R-eWAG.

R-eWAG Support for Local Configuration of GGSN IP Addresses

R-eWAG now has the ability to locally select a GGSN. This would be used in case a DNS server is unavailable or unreachable. A new CLI command is now available to locally configure GGSN IP address under the R-eWAG service.

Previous Behavior: Hidden test mode CLI command [ no ] ggsn-ip-address <ipv4_address> was available for this purpose.

New Behavior: Now new CLI command [ no ] gtp peer-ip-address <ipv4_address> can be used to locally configure GGSN IP address under the R-eWAG service. This CLI command is available only for the eWAG mode. The old CLI command [ no ] ggsn-ip-address <ipv4_address> is now removed for the eWAG mode.

R-eWAG Support for Alternate GGSN in Case Primary GGSN Rejects CPC

In case the DNS server returns more than one GGSN address for the given APN, and if CPC request to GGSN fails due to GGSN being unreachable, then next GGSN address from the list of addresses will be tried. Note that next GGSN addresses will also be tried in case GGSN rejects the CPC request due to one of the following reasons:

- No resources available
- All dynamic PDP addresses are occupied
- No memory is available
- Missing or unknown APN
- System failure
- Unknown PDP address or PDP type
- All decode errors at peer like “Mandatory IE incorrect”, “Mandatory IE missing”, “Optional IE incorrect”, and “Invalid message format”.


Next GGSN will be tried until either the address list is exhausted or PDP context activation succeeds. Note that R-eWAG is concerned with only first five reasons from the above list to retry with next GGSN. Maximum limit for the number of GGSN addresses that can be retried is 31.

**R-eWAG Support for CDR Functionality for Offline Charging**

R-eWAG now supports Offline Charging (CDR generation).

In offline charging, the charging information is collected concurrently with resource usage. This charging information is then passed through a chain of logical charging functions, and the CDR files are generated by the network, which are then transferred to the network operator's Billing Domain.

**R-eWAG Support for LI Functionality**

R-eWAG now supports Lawful Interception. The Lawful Intercept feature enables network operators to intercept subscriber control and data messages.

**R-eWAG Support for Enhanced Failure Handling**

R-eWAG now supports sending RADIUS DM with UE MAC-address when call setup fails due to auth failure, no resource, missing or unknown APN, and other reasons.
eWAG Command Changes as of September 30, 2013

This section provides information on eWAG command changes in release 15.0.

**Important:** For more information regarding commands in this section, refer to the *Command Line Interface Reference* for this release.

### New eWAG Commands

This section identifies new eWAG commands available in release 15.0.

**gtp peer-ip-address**

Use this command to configure the GGSN IP address under the eWAG service.
This command replaces the hidden mode command `[ no ] ggsn-ip-address <ipv4_address>.

```
configure
  context <context_name>
    ipsg-service <service_name> mode radius-server ewag [ -noconfirm ]
    gtp peer-ip-address <ipv4_address>
  no gtp peer-ip-address
end
```

**accounting-context**

This command allows to specify the GTPP accounting context.

```
configure
  context <context_name>
    ipsg-service <service_name> mode radius-server ewag [ -noconfirm ]
    accounting-context <context_name>
  no accounting-context
end
```

### Modified eWAG Commands

This section identifies eWAG commands modified in release 15.0.
None for this release.

 Deprecated eWAG Commands

This section identifies deprecated eWAG commands that are no longer supported in release 15.0.

**ggsn-ip-address**

The old hidden CLI command `[ no ] ggsn-ip-address <ipv4_address>` is now removed for the eWAG mode. The new CLI command `[ no ] gtp peer-ip-address <ipv4_address>` can be used to locally configure GGSN IP address under the eWAG service. This CLI command is available only for the eWAG mode.

```
[ no ] ggsn-ip-address <ipv4_address>
```
eWAG Performance Indicator Changes as of September 30, 2013

This section provides information on eWAG performance indicator changes in release 15.0.
None for this release.
This chapter identifies features and functionality added to, modified for, or deprecated from 15.0 Firewall software releases.

**Important:** All functionality from Limited Availability Release StarOS Version 14.1 has been included in General Availability Release StarOS Version 15.0. The *Cisco ASR 5x00 Release Change Reference, Version 14.1*, details new feature descriptions and configuration, performance, and security changes for the 14.1 release.
Firewall Enhancements for September 30, 2013

Firewall Feature Changes as of September 30, 2013

This section provides information on Firewall feature changes in release 15.0.

**Important:** For more information regarding features in this section, refer to the *Personal Stateful Firewall Administration Guide* for this release.

New Firewall Features

This section identifies new Firewall features available in release 15.0.

**Flooding Protection Support for Uplink flows**

Firewall flooding and port-scan protection is now supported for uplink-initiated flows in addition to downlink-initiated flows. This allows users to safeguard their own servers and hosts. Support to selectively enable this protection for specific servers is also provided. The `firewall dos-protection flooding` command is added in the Active Charging Service Configuration Mode in support of this feature.

**Server IP Address in Access Rule Definitions**

Access Rule Definitions now support Server IP address to avoid configuring multiple rule options as part of Firewall rules. With this release, the `ip server-ip-address` command is added in access ruledefs. If any address or host-pool range is specified as the server IP address, this address in the uplink direction will be treated as the destination address, and in downlink direction will be treated as the source address.

Modified Firewall Features

This section identifies Firewall features modified in release 15.0.

**SIP ALG Behavior**

As part of this feature, SIP ALG is made compatible with user-to-user authentication and processing 4xx responses as described in RFC 3261. A new command, `sip advanced` is added in the Active Charging Service Configuration mode to enable SIP ALG to maintain the same tag parameters (from and to tag) for Authorization or Proxy Authentication requests.

**Previous Behavior:** SIP ALG forwarded a re-invite request with credentials (sent by the client after the server responded with a 401 to the initial Invite request) with a new “From Tag” which is different from the “From Tag” added by SIP ALG for the initial Invite request. This was implemented as per section 19.3 of RFC 3261. As some SIP servers have strict policy implementations, calls are terminated due to this default behavior of SIP ALG.

**New Behavior:** In this release, the re-invite to 401 is sent with the same “From Tag” as the initial Invite request as defined in sections 8.1.3.5 and 22.2 of RFC 3261.
Firewall Command Changes as of September 30, 2013

This section provides information on Firewall command changes in release 15.0.

**Important:** For more information regarding commands in this section, refer to the Command Line Interface Reference for this release.

New Firewall Commands

This section identifies new Firewall commands available in release 15.0.

**firewall dos-protection flooding**

This command is configured to protect servers from mobile subscribers in uplink direction.

```bash
configure

active-charging service acs_service_name

firewall dos-protection flooding { { icmp | tcp-syn | udp } protect-servers { all | host-pool hostpool_name } packet limit packet_limit | inactivity-timeout timeout | uplink-sample-interval interval }

default firewall dos-protection flooding { icmp | tcp-syn | udp | inactivity-timeout | uplink-sample-interval }

no firewall dos-protection flooding { icmp | tcp-syn | udp }

end
```

**ip server-ip-address**

This command configures an access ruledef to analyze user traffic based on server IP address.

```bash
configure

active-charging service acs_service_name

access-ruledef access_ruledef_name

[ no ] ip server-ip-address { operator { ipv4/ipv6_address | ipv4/ipv6_address/mask } | { !range | range } host-pool host_pool_name }

der
```

**sip advanced**

This command enables SIP ALG to maintain the same tag parameters (from and to tag) for Authorization or Proxy Authentication requests.

```bash
configure
```
active-charging service acs_service_name
sip advanced out-of-dialog-request retain-tag
end

Modified Firewall Commands

This section identifies Firewall commands modified in release 15.0.

**show active-charging analyzer statistics**

This command displays statistical information for protocol analyzers. A filter based on instance is added to show the statistics of the number of SIP-TCP or SIP-UDP calls.

```
show active-charging analyzer statistics [ name protocol_name [ instance instance_number ] [ verbose ] ] [ | { grep grep_options | more } ]
```

**show active-charging firewall statistics**

This command displays Active Charging Stateful Firewall statistics. The `wide` keyword is added to display all available information in a single wide line.

```
show active-charging firewall statistics [ wide ]
```

**show active-charging flows**

This command displays information for active charging flows. New optional keywords `call-id`, `control-connection`, and `firewall` are added to this command as filters to debug Firewall enabled flows.

```
show active-charging flows { all | [ call-id call_id ] [ control-connection { ftp | pptp | rtsp | sip | tftp } ] [ firewall { not-required | required } ] }
```

**show active-charging flows**

This command displays information for active charging flows. New optional keywords `imsi`, `msisdn`, `binding-info`, and `username` are added to this command as filters to debug Firewall/NAT enabled flows.

```
show active-charging flows { all | [ imsi imsi_value ] [ msisdn msisdn_num ] [ nat { not-required | required [ binding-info ] } ] [ username user_name ] }
```

Deprecated Firewall Commands

This section identifies deprecated Firewall commands that are no longer supported in release 15.0.

None for this release.

Firewall Performance Indicator Changes as of September 30, 2013

This section provides information on Firewall performance indicator changes in release 15.0.
Firewall Changes in Release 15.0

Firewall Enhancements for September 30, 2013

Important: For more information regarding bulk statistics and output fields and counters in this section, refer to the Statistics and Counters Reference for this release.

New Firewall Bulk Statistics

This section identifies new Firewall bulk statistics available in release 15.0.

New in the Context Schema

The following bulk statistic is added in this release to display statistics for Firewall flows:
- sfw-current-flows

New in the ECS Schema

The following bulk statistics are added in this release to display statistics for SIP-TCP and SIP-UDP calls:
- sip-advanced-total-calls
- sip-advanced-udp-calls
- sip-advanced-total-udp-calls
- sip-advanced-tcp-calls
- sip-advanced-total-tcp-calls

Modified Firewall Bulk Statistics

This section identifies Firewall bulk statistics modified in release 15.0.
None for this release.

Deprecated Firewall Bulk Statistics

This section identifies Firewall bulk statistics modified in release 15.0.
None for this release.

New Firewall Output Fields and Counters

This section identifies new Firewall show command output fields and counters available in release 15.0.

show active-charging analyzer statistics name sip

The following fields have been added to the output of this command:
- Total SIP Calls
- Current SIP Calls
- Total SIP UDP Calls
- Current SIP UDP Calls
- Total SIP TCP Calls
- Current SIP TCP Calls

**show active-charging firewall statistics**

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

- Current Flows Processed by Firewall
- Current NAT Flows Processed by Firewall
- Current NAT44 Flows Processed by Firewall
- Current NAT64 Flows Processed by Firewall
- Current Bypass-NAT Flows Processed by Firewall
- Current Bypass-NAT44 Flows Processed by Firewall
- Current Bypass-NAT64 Flows Processed by Firewall

**show active-charging firewall statistics verbose**

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

- Current Flows Processed by Firewall
- Current NAT Flows Processed by Firewall
- Current NAT44 Flows Processed by Firewall
- Current NAT64 Flows Processed by Firewall
- Current Bypass-NAT Flows Processed by Firewall
- Current Bypass-NAT44 Flows Processed by Firewall
- Current Bypass-NAT64 Flows Processed by Firewall

**show active-charging sessions full**

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

- Firewall Policy IPv4
- Firewall Policy IPv6
- Bypass NAT Flow Present

**show active-charging subsystem all**

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

- SIP ALG Calls:
  - Total SIP ALG Calls
  - Current SIP ALG Calls
  - Total UDP SIP ALG Calls
  - Current UDP SIP ALG Calls
• Total TCP SIP ALG Calls
• Current TCP SIP ALG Calls

Modified Firewall Output Fields and Counters

This section identifies modified Firewall show command output fields and counters available in release 15.0.

show active-charging firewall statistics

The following fields have been modified in the output of this command:
• Total Bypass-NAT44 Flows Processed by Firewall (Total Bypass-NAT IPv4 Flows Processed by Firewall)
• Total Bypass-NAT64 Flows Processed by Firewall (Total Bypass-NAT IPv6 Flows Processed by Firewall)

show active-charging firewall statistics verbose

The following fields have been modified in the output of this command:
• Total Bypass-NAT44 Flows Processed by Firewall (Total Bypass-NAT IPv4 Flows Processed by Firewall)
• Total Bypass-NAT64 Flows Processed by Firewall (Total Bypass-NAT IPv6 Flows Processed by Firewall)

Deprecated Firewall Output Fields and Counters

This section identifies deprecated Firewall output fields and counters that are no longer supported in release 15.0.

show active-charging firewall statistics verbose

The following field has been deprecated:
• Packets Dropped due to No Ruledef in Rulebase

show active-charging firewall statistics callid <call_id> verbose

The following field has been deprecated:
• Packets Dropped due to No Ruledef in Rulebase

show active-charging firewall statistics domainname <domain_name> verbose

The following field has been deprecated:
• Packets Dropped due to No Ruledef in Rulebase

show active-charging firewall statistics username <user_name> verbose

The following field has been deprecated:
• Packets Dropped due to No Ruledef in Rulebase
Chapter 7
GGSN Changes in Release 15.0

This chapter identifies features and functionality added to, modified for, or deprecated from 15.0 GGSN software releases.

**Important:** All functionality from Limited Availability Release StarOS Version 14.1 has been included in General Availability Release StarOS Version 15.0. The *Cisco ASR 5x00 Release Change Reference, Version 14.1*, details new feature descriptions and configuration, performance, and security changes for the 14.1 release.

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:

- September 30, 2013, added *ACL Limit Behavior Change* under *Modified GGSN Features*

The following section points to the changes made in this document to correct omissions or technical errors made in the previously published *Release Change Reference* dated September 30, 2013:

- Command `gtpc supress nrupc` was mentioned as a deprecated command in the *Deprecated Commands* section. It has been made available now in the *GGSN Service Configuration Mode* commands chapter of *CLI Reference Guide*. 
GGSN Enhancements for February 27, 2015

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

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

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

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

---

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

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

---

**CSCun51617 - [gn-gp]: GGSN Not Informing PCRF about Network-Request-Support Change**

**Feature Changes**

**BCM Mode Derivation during gn-gp Handoff**

**Previous Behavior:** Earlier the UE support for bearer control mode (BCM) was unknown on handover from PGW to GGSN and therefore BCM would not be derived as expected.

**New Behavior:** With new changes, even if PCO IE is not sent in handover indication to GGSN but previously sent to PGW during call setup, BCM will be derived based on UE support in PGW.

**Customer Impact:** BCM mode will be derived based on UE and SGSN support on handover rather than assuming BCM in PGW to be always by UE.
**Feature Changes**

**Modified CPC Response of TEID**

**Previous Behavior:** The configured Newcall policy sent reject response before parsing the content (i.e. SGSN Control TEID IE) of CPC Req message. So, the response was sent with zero header TEID.

**New Behavior:** The CPC Req message will be parsed to search for SGSN Control TEID IE before Newcall policy is applied. The Header TEID of reject response will be received CPC Req Control TEID IE if it is valid else it will be zero.

**Customer Impact:** No Impact. The reject responses are sent with correct non-zero TEID if received correct value in CPC Req.
GGSN Enhancements for January 31, 2014

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

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

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

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

---

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

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

---

**CSCui12525 - BMC P-CSCF Discovery is not provided in CPC Response**

**Feature Changes**

**GGSN Support for IPv4 P-CSCF Discovery in CPC Request**

**Previous Behavior:** When PDP request was received with IPv4 P-CSCF address request in PCO, GGSN did not respond with P-CSCF address having configured on IMSA using PCSCF table CLI.

**New Behavior:** Support has been added for IPv4 P-CSCF request for GGSN product on similar line for IPv6 P-CSCF request.
CSCul65167 - ASR5K ECS Shaping of multiple torrent downloads

Feature Changes

Rule Matching for TCP Out-of-order (OOO) Failure Cases

Charging actions configured under ECS service for limiting P2P traffic throughput was not working as expected. While troubleshooting, it was found that when a single P2P download is performed, traffic is rate-limited correctly; however, when multiple downloads are done, rate limiting is not as configured anymore, and traffic starts exceeding the configured limit.

**Previous Behavior:** When TCP OOO packets were received and when there was any error in buffering those packets at ECS due to memory allocation failure, these packets were marked as TCP error packets and rule matching was done accordingly. TCP error was being set for packets when reordering timeout occurred.

**New Behavior:** TCP error will not be set now for TCP OOO packets when OOO timeout occurs or buffering fails due to memory allocation failures for those packets. Those packets will not match rules created for TCP error cases.

**Customer Impact:** If customer has configured TCP error related rules, then OOO timeout failure packets and memory allocation failure packets will not match these rules now. It will match normal TCP rules.

CSCul65556 - Sessmgr Crashes on seeing dhcpv6 server statistics

Feature Changes

Multiple DHCPv6 Calls Support

**Previous Behavior:** With the existing configuration, session manager used to crash and all the existing DHCPv6 and PD calls got released.

**New Behavior:** Obsolete CLIs have been removed from the configuration that led the Session Manager crash.

CSCul89329 - {AIS}dpca-custom24:call dropped if Supported-feature AVP absent in CCR-I

Feature Changes

dpca-Custom24 Release 8 Dictionary Support

**Previous Behavior:** If dictionary was Release 8 then it was mandatory to receive supported-feature from PCRF.

**New Behavior:** For dpca-custom24 which is also a Release 8 dictionary, call is not dropped if PCRF does not send supported feature in CCA-I, and configured value in PCEF is considered as received value.
GGSN Enhancements for November 30, 2013

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

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

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

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

---

**CSCui42540 - P-GW: DHCPv6 default UE prefix should be allocated from AAA and PD from DHCPv6**

**Feature Changes**

**DHCPv6 Default UE Prefix Allocated from AAA and PD from DHCPv6**

- **Previous Behavior:** Current implementation supports allocation of both default UE prefix and delegated prefixes from external DHCPv6 server.
- **New Behavior:** Added support for allocating default UE prefix from local/AAA and delegated prefix from external DHCPv6 server.

---

**CSCug55201: VZ BCPS QoS change; QCI<->MPLS EXP mapping for HA, UMTS-GGSN & eHRPD**

**Feature Changes**

**Set MPLS Experimental value for outbound traffic**

- **Previous Behavior:** Earlier the default behavior was to copy the DSCP value of mobile subscriber traffic to the EXP, if there was no explicit configuration for DSCP to EXP. It was done using the CLI `mpls map-dscp-to-exp dscp <n> exp <m>`.  
- **New Behavior:** A new CLI has been introduced which disables the default behavior and the EXP value is set to the configured `<value>`, if there is no explicit configuration of DSCP to EXP.

**Command Changes**

```bash
[ no ] mpls exp <value>
```
It is a new command added to set the default behavior as Best Effort using a zero value in the 3-bit MPLS EXP (Experimental) header. This setting overrides the value sent by the mobile subscriber.

```
configure
   context context_name
      [ no ] mpls exp <value>
   end
```

Notes:
- `<value>`
  Specifies the MPLS EXP header value as an integer from 0 through 7. Higher value indicates higher priority.
- `no`
  Reverts back to the default behavior, which is to copy the DSCP from the mobile subscriber packet to the EXP header of the packet, if there is no explicit configuration for DSCP to EXP.

**CSCuh73686 - GGSN: Modification of ‘timeout bearer-inactivity’ CLI to ignore default bearer**

**Feature Changes**

**Timeout Bearer Inactivity Feature**

**Previous Behavior:** The timeout bearer-inactivity CLI monitored all bearers on the PDN for inactivity. If the default bearer timed out unexpectedly, it caused the session to be torn down and the user was disconnected. This feature also looked at both uplink and downlink data.

**New Behavior:** The bearer inactivity timer can now be configured to exclude default bearer/primary bearer from monitoring bearer inactivity. In addition, this feature now has the option to look at either uplink or downlink data.

**Command Changes**

```
timeout bearer-inactivity
```

This command configures the bearer inactivity timer and the threshold value of the traffic through an APN.

New keywords have been added so the threshold value can now be configured for monitoring traffic at various levels. The bearer inactivity timer can also be configured to exclude default bearer/primary bearer from monitoring bearer inactivity.

```
configure
   context context_name
      apn apn_name
```
timeout bearer-inactivity seconds volume-threshold { downlink bytes | total bytes | uplink bytes }

timeout bearer-inactivity exclude-default-bearer

[ default | no ] timeout bearer-inactivity

diff
der  end

Notes:

- Only one threshold is allowed to be configured per APN which is to monitor total, uplink, or downlink traffic.
- Bearer inactivity timer is started only when time and volume threshold is configured.
- seconds must be an integer from 900 to 2592000. The minimum configurable value of bearer inactivity timer is reduced from 3600 seconds to 900 seconds.
- volume-threshold downlink: Threshold value of the downlink data traffic in a bearer.
- volume-threshold total: Threshold value of the uplink and downlink data traffic in a bearer.
- volume-threshold uplink: Threshold value of the uplink data traffic in a bearer.
- exclude-default-bearer: Ignore or exclude bearer inactivity handling for default/primary bearer.
- default | no: The bearer inactivity timer is disabled.
GGSN Enhancements for September 30, 2013

GGSN Feature Changes as of September 30, 2013

This section provides information on GGSN feature changes in release 15.0.

**Important:** For more information regarding features in this section, refer to the *GGSN Administration Guide* for this release.

**New GGSN Features**

This section identifies GGSN features and functionality added in release 15.0.

**3GPP TS 29.281 (GTPU) Release 10 Compliance**

The GGSN now complies to 3GPP TS 29.281 Rel-10. Support for UDP Port Extension header in Error indication message and Supported Extension Headers Notification message was added to become fully compliant with 3GPP Release 10.

Supported Extension Headers Notification message indicates a list of supported Extension Headers that the node can support. This message is sent only in case a GTP entity was required to interpret a mandatory Extension Header (by setting the comprehension required in extension header) but the GTP entity was not yet upgraded to support that extension header.

- If a Supported Extension Headers Notification is received from peer GTPU entity, node will not send the Extension Header to the peer entity.
- If a message which contains Extension Header is received from peer GTPU entity; if the extension header is set to comprehension required and the extension header cannot be interpreted by the node, it will send a Supported Extension Headers Notification message. This message shall include all the extension headers supported by the node.

UDP Port Extension header helps in handling the Error-Indication message efficiently. If any GTPU peer supports this extension header, then sending this extension header in Error-Indication message will help in processing the Error-Indication message.

With the support for Supported Extension Headers Notification message it helps notifying the GTPU peer about the GTPU capabilities of the node. This message is sent only in case the node was required to interpret a mandatory Extension Header (by setting the comprehension required in extension header) but the node was not yet upgraded to support that extension header.

**DSCP Marking - GTP-U on per APN Basis**

**Previous Behavior:** Prior to release 15.0, DSCP marking table was configured on GGSN service level.

**New Behavior:** From release 15.0 onward, CLI is added to associate the qos-qci-mapping table in APN.

This feature provides the flexibility to have a different DSCP marking table on per APN basis so that traffic on each of the APNs can be marked differently, depending on the needs of the APN.
The GGSN supports configurable DSCP marking of the outer header of a GTP-U tunnel packet based on a QCI/THP table for the S5/S8 and Gn/Gp interfaces. This feature allows configuring DSCP marking table on a per APN basis.

In order to be backward compatible with old configuration, if a DSCP marking table is associated with GGSN service and not with the APN, then the one in GGSN service will be used. If table is associated in both GGSN service and APN, then the one on APN will take precedence.

Refer to the GGSN Command Changes section for the new CLI.

**DHCPv6 Prefix Delegation**

**Previous Behavior:** DHCPv6 Prefix delegation was not supported on GGSN prior to release 15.0

**New Behavior:** From 15.0 onward GGSN supports DHCPv6 Prefix Delegation.

DHCPv6 prefix delegation is required to support deployment models where multiple IPv6 prefixes can be delegated to the UE and which can be further subnetted by the UE and assigned to the links in its internal network. UE will act as an IPv6 router here and will be responsible for just prefix delegation or for prefix delegation along with address assignment and other configuration information. DHCPv6 prefix delegation will allow prefixes to be delegated to the UE independent of bearer establishment and thus without requiring any changes to the mobility signaling protocols.

Refer to the GGSN Command Changes section for the new CLI.

**GTP Throttling**

**Previous Behavior:** Prior to 15.0, the GGSN was not supporting GTP throttling.

**New Behavior:** From 15.0 onward, the GGSN supports PDP throttling to help control the rate of incoming/outgoing messages on GGSN. This functionality is used in ensuring GGSN doesn’t get overwhelmed by the GTP control plane messages. Also it will help in ensuring the GGSN will not overwhelm the peer GTP-C node with GTP Control plane messages.

This feature covers over-load protection of GGSN nodes and other external nodes with which it communicates.

External node overload can happen in a scenario where GGSN generates signaling requests at a higher rate than other nodes can handle. Also if the incoming rate is high at GGSN node, we might flood any of the external nodes. Hence throttling of both incoming and outgoing control messages is required.

**Important:** GTP throttling will be done only for session level control messages. Path management messages will not be rate limited.

Refer to the GGSN Command Changes section for the new and modified CLIs.

**Important:** This feature is license dependent. Please contact your local sales representative for more information.

**Network Mobility (NEMO) Support**

**Previous Behavior:** NEMO (NEtwork MObility) provides wireless connectivity between enterprise core network and remote sites over 3G/4G network. The wireless connection can be used as either primary link or backup link. All the hosts in the remote site can directly communicate with hosts in the core network without using NAT.

Enterprise VPN service is one of the main use case for this feature. Fast deployment, flexible bandwidth arrangement for customers are some of the advantages of this service. Customers include banks, financial institutions, multi-sited
enterprises, city public safety departments, transportation fleet, etc. This is becoming a new revenue source for network operators, and thus the need to support this feature is gaining momentum.

NEMO was not supported on GGSN for 3G (UMTS/GERAN) access.

**New Behavior:** From 15.0 onward GGSN supports standard based NEMO feature on ASR5x00 platform. It allows Operators to support Enterprise VPN service with the advantage of faster deployment and flexible bandwidth arrangement for customers.

Refer to the *GGSN Command Changes* section for the new CLI.

---

**Important:** This feature is license dependent. Please contact your local sales representative for more information.

### Peer GTP Node Profile Configuration Support

**Previous Behavior:** Prior to 15.0, the GGSN service allows operator to configure list of SGSNs. Using this configuration, operator can also control some parameters associated with the configured SGSN; like RAT type. This would be taken from configuration, if CPC request doesn’t have RAT type.

**New Behavior:** From 15.0 onward, the GGSN service supports the peer profile to allow flexible profile based configuration to accommodate growing requirements of customizable parameters with default values and actions for peer nodes of GGSN. With this feature configuration of GTPC parameters and disabling/enabling of Lawful intercept per MCC/MNC or IP address based on rules defined.

With support of this functionality the GGSN service supports the peer profile to allow flexible profile based configuration to accommodate growing requirements of customizable parameters with default values and actions for peer nodes of GGSN. With this feature configuration of GTP-C parameters and disabling/enabling of Lawful intercept per MCC/MNC or IP address based on rules can be defined.

A new framework of peer-profile and peer-map is introduced for configuration. Peer-profile configuration captures the GTP-C specific configuration and/or Lawful Intercept enable/disable configuration. GTP-C configuration covers the configuration of GTP-C retransmission (maximum number of retries and retransmission timeout) and GTP echo configuration.

Peer-map config matches the peer-profile to be applied to a particular criteria. Peer-map supports criteria like MCC/MNC (PLMN-ID) of the peer or IP-address of the peer. Peer-map can then be associated with GGSN service.

With support of this feature the Operators can configure a profile which can be applied to a specific set of peers. For example, have a different retransmission timeout for foreign peers as compared to home peers.

Refer to the *GGSN Command Changes* section for the new CLI.

### Modified GGSN Features

This section identifies GGSN features modified in release 15.0.

### 3GPP Tracing to Intercept Random Subscriber

**Previous Behavior:** The current session trace feature is either signaling or management based which is very specific to particular subscriber. The requirement is to trace the random subscriber which is not just explicitly linked or identified by IMSI in GTP messages or configured through CLI.

**New Behavior:** With this enhancement the 3GPP tracing will be enhanced to intercept random subscriber with this feature the operator can trace the random subscriber which is not just explicitly linked or identified by IMSI in GTP messages or configured through CLI.
The session trace is activated on demand for a limited period of time for specific analysis purposes. The maximum limit will restrict on the number of random subscriber tracing. Random session trace will be given priority over signaling and management based session trace.

Earlier in order to enable trace subscribers, the identifier like IMSI was mandatory. But there are scenario where Operators want to enable the trace without knowing the subscriber id. Cases like Operator wanting to monitor the next ‘n’ number of calls, or monitor subscribers in a particular IMSI range are some use cases now which are possible with this enhancement. This cab be provisioned by tools like Cisco InTracer.

The valid combinations of Session Trace types per service (Network element) are:

- Signaling only
- Management only
- Random only
- Management and Signaling
- Management and Random

Refer to the GGSN Command Changes section for the new CLI.

**3GPP TS 29.281 (GTPU) Release 10 Compliance**

**Previous Behavior:** GGSN was not fully compliant to 3GPP TS 29.281 Rel-10 to support UDP Port Extension header in Error indication message and Supported Extension Headers Notification message.

**New Behavior:** This feature enhances the GTPU capabilities of GGSN and PGW in compliance to 3GPP TS 29.281 Rel-10. Support for UDP Port Extension header in Error indication message and Supported Extension Headers Notification message was added to become fully compliant with 3GPP Release 10.

Supported Extension Headers Notification message indicates a list of supported Extension Headers that the node can support. This message is sent only in case a GTP entity was required to interpret a mandatory Extension Header (by setting the comprehension required in extension header) but the GTP entity was not yet upgraded to support that extension header.

- If a Supported Extension Headers Notification is received from peer GTPU entity, node will not send the Extension Header to the peer entity.
- If a message which contains Extension Header is received from peer GTPU entity; if the extension header is set to comprehension required and the extension header cannot be interpreted by the node, it will send a Supported Extension Headers Notification message. This message shall include all the extension headers supported by the node.

UDP Port Extension header helps in handling the Error-Indication message efficiently. If any GTPU peer supports this extension header, then sending this extension header in Error-Indication message will help in processing the Error-Indication message.

With the support for Supported Extension Headers Notification message it helps notifying the GTPU peer about the GTPU capabilities of the node. This message is sent only in case the node was required to interpret a mandatory Extension Header (by setting the comprehension required in extension header) but the node was not yet upgraded to support that extension header.

**ACL Limit Behavior Change**

A 16 ACL limit for redirect-css is now removed and a generic limit for ACL is applied.

**DNS Support for IPv4/IPv6 PDP Contexts**
**Previous Behavior:** GGSN was supporting DNS for IPv4 PDP context only.

**New Behavior:** This feature will enhance the DNS support for IPv4/IPv6 PDP Context in GGSN. In this feature MS may request for DNS server IPv4 or IPv6 addresses using the Protocol Configurations Options IE (as a container or as a part of IPCP protocol configuration request), in PDP Context Activation procedure, for PDP Type IPv4, IPv6 or IPv4v6. In that case, the GGSN, may return the IP address of one or more DNS servers in the PCO IE, in the PDP Context Activation Response message. The DNS address(es) shall be coded in the PCO as specified in 3GPP TS 24.008. This is as per the CR number 1344 for 3GPP TS 24.008.

Refer the GGSN Administration Guide for configuration example.

### Enhancement to Simultaneous 3GPP Tracing

**Previous Behavior:** Prior to 15.0, the simultaneous 3GPP trace limit was 30 sessions.

**New Behavior:** From 15.0 onward, the 3GPP tracing limit is enhanced to support simultaneous traces from 30 to 1000. The generated trace files are forwarded to external trace collection entity at regular intervals through (S)FTP if ‘push’ mode is enabled. If the push mode is not used, the files are stored on the local hard drive and must be pulled off by the TCE using FTP or SFTP.

### Report Subscriber Summary per GTP-U Address

**Previous Behavior:** GGSN was not supporting the CLI to list the number of sessions per GTPU local addresses in a Gateway.

**New Behavior:** This feature enhances the existing CLI `show gtpu` and `show gtpu statistics` with new keyword `local address` to list the number of sessions per GTPU local addresses in a Gateway. To support load balancing GTPU module distributes the session across multiple local IP addresses for a single eGTPC control plane IPv4 or IPv6 address.

Refer to the *GGSN Command Changes* section for the new CLI.

### Deprecated GGSN Features

None for this release.

### GGSN Command Changes as of September 30, 2013

This section provides information on GGSN command changes in release 15.0.

**Important:** For more information regarding commands in this section, refer to the *Command Line Interface Reference* for this release.

### New GGSN Commands

This section identifies new GGSN commands available in release 15.0.

**associate qci-qos-mapping**

New command for GGSN is added in the APN configuration mode to associate the preconfigured QCI-QoS-mapping table with an APN for per APN basis DSCP marking.
configure

context ctx_name

apn apn_name

associate qci-qos-mapping qci_qos_map_table_name

end

Notes:
- The qci_qos_map_table_name identifies a pre-configured QCI-QoS-Mapping table defined with commands in the QCI-QoS-Mapping configuration mode.

gtpc overload-protection egress

New command is added in the Context configuration mode to enable outgoing control message throttling.

configure

context ctx_name

[ no ] gtpc overload-protection egress rlf-template rlf_tmplt_name

end

gtpc overload-protection ingress

New command is added in the Context configuration mode to enable incoming control message throttling.

configure

context ctx_name

[ no ] gtpc overload-protection ingress msg-rate msg_rate [ delay-tolerance msg_queue_delay] [ queue-size queue_size ]

end

peer-profile

A new command, peer-profile, is added to the Global configuration mode to provide access to commands that configure the peer GTP node profile parameters.

To access the configuration commands for the GGSN peer profile, the user must use the ggsn-access option for the service-type keyword.

The Peer-Profile Configuration Mode includes the following commands to configure the parameters for a specific peer-profile:

- description
- gtpc

Use the following example to guide your use of these new commands:

configure
peer-profile service-type ggsn-access { default | name peer_profile_name }

description desc_string
gtpc { echo [ interval inter_dur | retransmission-timeout echo_retrans_dur ] | max-retransmission retrans_num | retransmission-timeout retrans_dur }

end

permission nemo

New command is added to support NEtwork MObility (NEMO) functionality with an APN on a GGSN node.

configure

context <context_name>

apn apn_name

[ no | default ] permission nemo
end

prefix-delegation

New prefix-delegation command allows the operator to configure the prefix lifetime parameters that can be used by a particular DHCPv6 service for delegated prefixes.

configure

context ctx_name

dhcpv6-service dhcpv6_svc_name

dhcpv6-server

prefix-delegation valid-lifetime valid_lifetime preferred-lifetime pref_lifetime

end

rlf-template

This new command has been added to the Global configuration mode to access the RLF Template configuration mode. The following commands are added in the RLF-Template configuration mode to define the throttling parameters:

- delay-tolerance
- msg-rate
- threshold

To configure the generic rate-limit function template use the following configuration example:

configure

rlf-template rlf_tmplt_name
delay-tolerance tolerance_value
msg-rate tps_value burst_size burst_size
threshold [ lower lower_thresh_limit | upper upper_thresh_limit ]
end

session trace random

New session trace random command is added to the Exec Mode to enable or disable the subscriber session trace functionality based on a random trace on the network element. If enabled, the subscriber selection will be based on random logic on all instances of sessions on a specified UMTS/EPS network element. This command also clears/resets the statistics collected for subscriber session trace on a system.

[ no ] session trace random random_num network-element { ggsn | pgw } [ interface { all | interface } ]

session trace signaling

New session trace signaling command is added to the Exec Mode to enable or disable the subscriber session trace functionality based on signaling information on one or all instances of the session on a specified UMTS/EPS network element. It also clears/resets the statistics collected for subscriber session trace on a system.

[ no ] session trace signaling network-element { ggsn | pgw }

Modified GGSN Commands

This section identifies modified GGSN commands available in release 15.0.

ipv6 address alloc-method

This command allows the operator to configure the IPv6 address allocation and DHCPv6 prefix-delegation support for an APN. With this release, an optional filter allow-prefix-delegation is added for use with the dhcpv6-proxy keyword in the APN configuration mode.

configure
    context ctx_name
    apn apn_name
    ipv6 address alloc-method dhcpv6-proxy allow-prefix-delegation
end

ipv6 address prefix-delegation-len

This command allows the operator to configure the prefix length (48/52/56 bit length) per-APN for DHCPv6 prefix-delegation support. With this release, the prefix-delegation-len keyword is added to the ipv6 address command in the APN configuration mode.

configure
context  ctx_name
  apn  apn_name
      [  no ] ipv6 address prefix-delegation-len { 48 | 52 | 56 }
  end

show gtpu
To view the local addresses bound to GTPU sessions, the new local-address keyword is added to the existing command.

show gtpu local-address

show gtpu statistics
To view the enhanced information for the number of sessions per GTPU for local-addresses the new filter keyword local-address is added to the existing command.

show gtpu statistics local-address <ip_address>

Deprecated GGSN Commands
This section identifies deprecated GGSN commands available in release 15.0.

gtpc suppress-nrupc
This command enables and disables NRUPC suppression on CPC for QoS change.

configure
  context <context_name>
      ggsn-service <ggsn-svc>
      [  no ] gtpc suppress-nrupc { cpc | upc } qos-change
  end

GGSN Performance Indicator Changes as of September 30, 2013
This section provides information on GGSN performance indicator changes in release 15.0.

Important: For more information regarding bulk statistics in this section, refer to the Statistics and Counters Reference for this release.

New GGSN Bulk Statistics
This section identifies new GGSN bulk statistics available in release 15.0.
None for this release.

**Modified GGSN Bulk Statistics**

This section identifies GGSN bulk statistics modified in release 15.0.

None for this release.

**Deprecated GGSN Bulk Statistics**

This section identifies GGSN bulk statistics deprecated in release 15.0.

None for this release.

**New GGSN Output Fields and Counters**

This section identifies new GGSN show command output fields and counters available in release 15.0.

`show subscribers ggsn-only full all`

The following counters have been added to display authorized QoS Policy parameters:

- PCRF Authorized Bearer QoS
  - QCI
  - ARP
  - PCI
  - PL
  - PVI
  - MBR uplink (bps)
  - MBR downlink (bps)
  - GBR uplink (bps)
  - GBR downlink (bps)
  - APN AMBR uplink (bps)
  - APN AMBR downlink (bps)
Chapter 8
GTPP Changes in Release 15.0

This chapter identifies GTPP management features and functionality added to, modified for, or deprecated from the 15.0 software releases.


Important: Enhancements to SNMP MIBs in release 15.0 are located in the SNMP MIB Changes chapter. Enhancements to Web Element Manager (WEM) in release 15.0 are located in the Web Element Manager Changes chapter.
GTPP Enhancements for April 30, 2014

This section identifies all of the 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 *ASR 5x00 Command Line Interface Reference* for this release.

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

CSCul77461 - aaaproxy in warn state during call model run

**Feature Changes**

**Limited GTPP Group Configuration for APN**

The AAA proxy allocates a lot of memory on a per GTPP group basis statically regardless of the usage. So if the number of GTPP groups is reduced to around 3 then the issue with the AAA proxy going to warn memory state will not be observed.

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

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

**Customer Impact:** On an analysis, it is determined that customers have not yet exceeded a maximum of six GTPP groups in the configuration. With the reduction in the number of GTPP groups configured, there will no CDR loss due to AAA proxy kill as CDRs are archived in AAA manager when AAA proxy goes to warn state.
GTPP Enhancements for January 31, 2014

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 *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.

CSCty15478 - [GTP-S5]Gz: Cause to be 'Mngmnt-Intervntn' on clearing call from box

**Applicable Products:** P-GW

**Feature Changes**

**Change in Value of CDR Element “CauseforRecordClosing”**

**Previous Behavior:** When a call is cleared from the chassis, the field “causeForRecordClosing” in a PGW-CDR shows “Normal Release”.

**New Behavior:** In this release, the behavior has been changed to comply with 3GPP specifications. That is, the default “causeForRecordClosing” in PGW-CDR will be “Management Intervention”. To support this, a new CLI has been provided to control the value of “causeForRecordClosing” of PGW-CDR when a call is cleared from the chassis.

*CSCty15478 - [GTP-S5]Gz: Cause to be 'Mngmnt-Intervntn' on clearing call from box*

**Important:** This behavioral change is limited to PGW-CDR Release 8 dictionaries only.

**Customer Impact:** A new CLI is being provided, which will allow the customer to control the value of the CDR element “CauseforRecordClosing”. When this CLI is configured the CauseforRecordClosing will be Normal-Release. This CLI can be configured or changed on the fly.

**Command Changes**

`gtpp egcdr`

A new keyword has been added to control the configuration of “causeForRecordClosing” in PGW-CDR when a call is cleared from the chassis.

```
cfg
   context context_name
   gtpg gtpg_name
```
**CSCui40165 - Charging in ‘servers unreachable’ state, special reporting in CDRs**

Applicable Products: P-GW

Feature Changes

Secure Charging Functionality During OCS Failure

This feature provides the functionality to generate interim PGW-CDRs with the following causeForRecordClosing Reasons:

- OCS_UNREACHABLE – when OCS becomes unreachable.
- OCS_REACHABLE – when OCS becomes reachable.
- OCS_STATUS_UNKNOWN – when a session is terminated and when there is a chance of double counting. Scenario in which this will be used is when the configured interim-quota is exhausted and when the connection to the server is retried by sending out a CCR-I/U and termination is initiated (before timeout).

The duplicate charging is solved by suppressing the MSCC’s in CCR-T. Since no MSCCs are encoded in the CCR-T, no usage will be reported and at the same time a CCR-T will be generated to close the session on the OCS server.

**Important:** This behaviour is applicable only for custom45 GTPP dictionary (PGW-CDRs).

For this feature to work, custom45 should be configured as the GTPP dictionary under GTPP Group configuration and the CLI command “servers-unreachable” should also be configured under Credit-Control Group. With this feature turned on, it is easy to identify the potentially unreported usage prior to the CCFH.

There will NO OCS_UNREACHABLE CDR generations on failed retries, when we are in unreachable state.

There will be no flag in the CDRs to indicate if the OCS is unreachable/reachable. So, the CDRs generated due to other reasons like time-limit, volume-limit, triggers, etc., while the OCS is unreachable, will have no flag indicating the OCS-unreachable status. If there are no specific service-condition changes to be reported, the LOSDVs that are cut by these CDRs (Unreachable/Reachable/OCS_STATUS_UNKNOWN) will have record-closure as the serviceConditionChange.

**CSCuj99515 - Disabling the triggers for closing CDR service containers**

Applicable Products: P-GW
Feature Changes

Suppression of LOSDV Addition Trigger Generated for DCCA and Service Idle Out Triggers

**Previous Behavior:** CLI was not available to disable DCCA and service-idle out triggers for CDR generation.

**New Behavior:** With this release, configurable options are provided to disable the addition of LOSDV in PGW-CDR for DCCA generated triggers and when a service idles out.

Command Changes

gtp trigger

Two new keywords options “service-idle-out” and “dcca” are added to the GTPP Group configuration to provide an option to disable the closure of Service container for PGW-CDRs.

```bash
configure

context <context_name>

gtpp group <gtpp_grpname>

gtpp trigger { service-idle-out | dcca }

no gtpp trigger { service-idle-out | dcca }

end
```

CSCul86799 - AAA side changes for S-CDR should quantify the volume drop with counter

**Applicable Products:** SGSN

Feature Changes

New S-CDR Field in custom33 Dictionary

A new CDR field “sgsn2gDlDroppedBytes” has been added to custom33 GTPP dictionary to address the SGSN and GGSN CDR packet count mismatch issue occurred due to paging failure and queue full in 2G scenario.

This is an optional field present only in the 2G S-CDRs to indicate the number of 2G bytes dropped by the SGSN. Note that this is not a CLI controlled feature.

This field is provided also for partial CDRs generated with gtpp interim, volume trigger, time tarrif, etc.
GTPP Enhancements for November 30, 2013

This section identifies all of the GTPP dictionary and CDR 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 *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.

**CSCuf51057 - IPv6 Prefix**

**Applicable Products:** P-GW

**Feature Changes**

**IPV6 Prefix Changes**

**Previous Behavior:** Support was available only for /64 prefix length. Hence, the “servedPDPPDNAddress” attribute did not include a prefix field in the PGW-CDR.

**New Behavior:** /56 /52 and /48 prefix lengths will be supported by ECS in addition to /64. So, the “servedPDPPDNAddress” attribute may have a prefix length field in the PGW-CDR.

**Important:** The CDR attribute field “servedPDPPDNAddressExt” is available if enabled by configuration. This is necessary for full support of IPV6 and dual stack.

Additionally, when the CLI “gtpp attribute served-pdp-pdn-address-prefix-length” is configured, the servedPDPPDNAddress field will support reporting the IPv6 prefix length as outlined in 3GPP 32.298 standard spec. The prefix length will only be reported if:

- it is configured
- it is not the default length of 64
- it is an IPv6 or IPv4v6 call
**GTPP Enhancements for September 30, 2013**

This section provides information on GTPP accounting management changes available in release 15.0.

---

**Important:** For more information regarding GTPP dictionaries and CDRs mentioned in this section, refer to the *GTPP Interface Administration and Reference* for this release.

---

**GTPP Feature Changes**

This section identifies GTPP feature changes available in release 15.0.

**New GTPP Features**

This section identifies new GTPP features available in release 15.0.

**AAA Changes To Support Location Services (LCS) Feature**

**Applicable Product(s):** SGSN

The Location Services (LCS) feature in SGSN provides the mechanism to support mobile location services for operators, subscribers and third party service providers. AAA changes have been made to support the LCS feature. A new CDR type Mobile Originated Location Request CDRs (LCS-MO-CDR) is introduced. LCS-MO-CDRs support the standard dictionaries.

For detailed information on LCS-MO-CDRs, refer to the *Cisco ASR 5x00 GTPP Interface Administration and Reference*.

**GTPP Attribute Configuration Support for GGSN**

**Applicable Product(s):** GGSN

Configuration support is provided for GGSN to include the following GTPP attributes in the CDR request:

- Apn-ni
- Apn-Selection-Mode
- Pdp-Type
- Pdp-Address

This enhancement reduces the need for creating new dictionaries as CLI control is available for GTPP attributes.

**GTPP Attribute Configuration Support for S-GW**

**Applicable Product(s):** S-GW

Configuration support is provided for S-GW to include the following GTPP attributes in the CDR request:

- Apn-ni
- Apn-Selection-Mode
This enhancement reduces the need for creating new dictionaries as CLI control is available for GTPP attributes.

New GTPP Dictionary for Compatibility with 3GPP Release 10

For the compliance of CDRs with 3GPP Release 10 requirements, this new GTPP dictionary “custom35” has been provisioned. This dictionary currently supports only PGW-CDRs. The custom35 contains all the PGW-CDR dictionary as implemented in custom34, and adds a set of attributes from TS 32.298 v10.7. Each new attribute can be individually CLI controlled on custom35. The default behavior is to not include the attributes if not configured.

Note these new attributes and their associated CLI will have no effect on other dictionaries, including custom34.

SGW-CDR Configurable Option

**Applicable Product(s):** S-GW

As part of this feature, new CLI options were added in GTPP Group Configuration mode to enable controlling whether the APN-AMBR attribute needs to be sent in SGW-CDR or not and/or even control the trigger for container creation.

Configuration is added to control sending the APN-AMBR attribute information in SGW-CDRs for all bearers, default bearer, or non-GBR bearers.

Configuration is also added to control trigger for container addition in case of any change in APN-AMBR.

Suppression of Zero Volume CDRs

**Applicable Product(s):** GGSN, P-GW, SGSN, S-GW

**Important:** The Zero Volume CDR Suppression is a license-controlled feature. For more information, contact your Cisco account representative.

This feature allows the customers to suppress the CDRs with zero byte data count, so that the OCG node is not overloaded with a flood of CDRs. To support this, a new CLI command “gtpp suppress-cdrs zero-volume { final-cdr | internal-trigger-cdr | external-trigger-cdr }” has been added in the GTPP Group configuration mode.

The CDRs can be categorized as follows:

- **final-cdr:** These CDRs are generated when the session ends.
- **internal-trigger-cdr:** These CDRs are generated due to internal triggers such as volume limit, time limit, tariff change or user generated interims through the CLI commands.
- **external-trigger-cdr:** These CDRs are generated due to external triggers such as QoS Change, RAT change and so on. All triggers which are not considered as final-cdrs or internal-trigger-cdrs are considered as external-trigger-cdrs.

Customers can select the CDRs they want to suppress. This feature is disabled by default to ensure backward compatibility.
Modified GTPP Features

This section identifies GTPP features modified in release 15.0.

AF Charging Identifier Information in PGW-CDRs

**Applicable Product(s):** P-GW

**Previous Behavior:** AF Charging Identifier was not getting populated in PGW-CDR.

**New Behavior:** The AF Charging ID is now included in the LOSDV field of PGW-CDRs when the GTPP dictionary “custom34” is used.

Change in the Format of QoS Field

To support the implementation of custom35 dictionary for 3GPP Rel.10, the format of QoS field is changed from 3G to EPS.

The 3GPP TS 32.298 v10.7 specifies EPCQoSInformation format for qosInformationNeg. The EPCQoSInformation is now aligned with the definition in TS 29.212.

This also adds the APN Aggregate Max Bit Rate Uplink and Downlink. This format is controlled by the “gtpp attribute apn-ambr” CLI which currently exists for custom24.

GTPP Secondary Group Configuration for P-GW

**Applicable Product(s):** P-GW

**Previous Behavior:** When LTE-only core was used without GGSN, secondary GTPP group was not possible to be configured under APN for P-GW without GGSN license. The license was enabled only for GGSN and not for P-GW.

**New Behavior:** This feature enables license for P-GW to allow configuring secondary GTPP group under APN.

IPv6 Prefix Length in servedPDPPDNAddress Field

**Applicable Product(s):** P-GW

**Previous Behavior:** Served IMSI IPv6 address did not have a prefix field in the PGW-CDR.

**New Behavior:** The IPv6 prefix is now included in Served PDP Address or Served PDP/PDN Address field in the PGW-CDRs. When configured via “gtpp attribute served-pdp-pdn-address-prefix-length”, the servedPDPPDNAddress field supports reporting the IPv6 prefix length as outlined in 32.298. The prefix length will only be reported if –
- it is configured
- it is not the default length of 64
- it is an IPv6 or IPv4v6 call

RAN and NAS Cause Code Private Extensions in PGW-CDR

**Applicable Product(s):** P-GW

**Previous Behavior:** RAN and NAS cause codes were not getting populated in PGW-CDR when delete bearer command was received.

**New Behavior:** Support is provided to include RAN and NAS cause codes in PGW-CDR in the GTPP dictionary “custom34” during delete bearer command.
Unauthenticated IMSI Field in PGW-CDRs

Applicable Product(s): P-GW

Previous Behavior: There was no support for the field “IMSI Unauthenticated Flag” in the P-GW record.

New Behavior: Upon detecting a subscriber with unauthorized IMSI, this field “IMSI Unauthenticated Flag” if configured will be present in the PGW-CDRs in custom35 GTPP dictionary.

This field can be configured using the command `gtpp attribute imsi-unauthenticated-flag` in the GTPP Group Configuration mode.

GTPP Command Changes

This section identifies GTPP command changes available in release 15.0.

**Important:** For more information regarding commands in this section, refer to the Command Line Interface Reference for this release.

New GTPP Commands

This section identifies new GTPP commands available in release 15.0.

`gtpp suppress-cdrs zero-volume`

Applicable Product(s): GGSN, P-GW, SAEGW, SGSN, S-GW

This command is used to suppress the CDRs (G-CDRs, eG-CDR, PGW-CDRs, SGW-CDRs, SGSN CDRs) with zero byte data count.

**Important:** The Zero Volume CDR Suppression is a license-controlled feature. For more information, contact your Cisco account representative.

```
configure

    context context_name

    gtppp group group_name

    gtppp suppress-cdrs zero-volume { final-cdr | internal-trigger-cdr | external-trigger-cdr } +

    { default | no } gtppp suppress-cdrs zero-volume

end
```

Customers can select the CDRs they want to suppress. This feature is disabled by default to ensure backward compatibility.
Modified GTPP Commands

This section identifies GTPP commands modified in release 15.0.

accounting

Applicable Product(s): SGSN

The `accounting` command in GPRS Service Configuration Mode and SGSN Service Configuration Mode has been updated to include a new keyword `lcs mo-cdr`, to enable/disable the generation of LCS-MO-CDRs.

configure

```
context context_name

gprs-service service_name

accounting { cdr-types { mcd | scd | sms { mo-cdr | mt-cdr } | lcs { mt-cdr | mo-cdr } | smbmscdr }+ | context cntx_name }

end
```

config

```
context <context_name>

sgsn-service service_name

accounting { cdr-types { mcd | scd | sms { mo-cdr | mt-cdr } | lcs { mt-cdr | mo-cdr } | smbmscdr }+ | context cntx_name }

end
```

gtppp attribute

Applicable Product(s): P-GW

This command has been enhanced to enable the attribute fields in the CDRs (PGW-CDRs). This feature is implemented to maintain the CDRs to be compliant with 3GPP Release 10 requirements.

configure

```
context context_name

  gtpp group group_name

  gtpp attribute { dynamic-flag-extension | imsi-unauthenticated-flag | served-pdp-pdn-address-prefix-length } +

  { default | no } gtpp attribute { dynamic-flag-extension | imsi-unauthenticated-flag | served-pdp-pdn-address-prefix-length } +

end
```
Note that, if configured, these attribute fields will be present in the PGW-CDRs in custom35 dictionary.

**gtpp attribute**

This command controls the inclusion of APN AMBR information in SGW-CDRs for all bearers, default bearer, or non-GBR bearers based on the configurations.

```
configure
  context context_name
  gtpp group group_name
  gtpp attribute apn-ambr [ include-for-all-bearers | include-for-default-bearer | include-for-non-gbr-bearers ]
    { default | no } gtpp attribute apn-ambr [ include-for-all-bearers | include-for-default-bearer | include-for-non-gbr-bearers ]
end
```

For backward compatibility, the attribute is not supported for custom11 dictionary. The attribute is absent in SGW-CDR for custom34 because the EPCQoS attribute in which AMBR values are to be added is absent. Therefore, the values for AMBR are also not seen in this case.

**gtpp trigger**

This command allows user to add CDR containers in SGW-CDRs for all bearers, default bearer, or non-GBR bearers based on the configurations.

The first container of each CDR includes APN-AMBR fields along with QoS. In the following containers this field is present if previous change condition is “QoS change” or “APN AMBR Change”.

```
configure
  context context_name
  gtpp group group_name
  gtpp trigger apn-ambr-change [ default-bearer-only | all-non-gbr-bearers | all-bearers ]
    { default | no } gtpp trigger apn-ambr-change [ default-bearer-only | all-non-gbr-bearers | all-bearers ]
end
```

**Deprecated GTPP Commands**

This section identifies deprecated GTPP commands that are no longer supported in release 15.0.

None for this release.
GTPP Dictionary Changes

This section identifies GTPP dictionary changes available in release 15.0.

**Important:** GTPP interface CDR field descriptions for dictionaries are located in the *GTPP Interface Administration and Reference* for this release.

New GTPP Dictionaries

This section identifies new GTPP dictionaries in release 15.0.
The following dictionary has been added in this release for P-GW:
- custom35

Modified GTPP Dictionaries

This section identifies GTPP dictionaries modified in release 15.0.
The following dictionary has been modified in this release:
- custom34 – Includes RAN and NAS cause codes in PGW-CDR

Deprecated GTPP Dictionaries

This section identifies deprecated GTPP dictionaries that are no longer supported in release 15.0.
None for this release.

GTPP Performance Management Changes

This section identifies GTPP performance management changes available in release 15.0.

**Important:** For more information regarding bulk statistics in this section, refer to the *Statistics and Counters Reference* for this release. For more information regarding commands in this section, refer to the *Command Line Interface Reference* for this release.

New GTPP Bulk Statistics

This section identifies new GTPP bulk statistics available in release 15.0.

New in the GTPP Schema

**Applicable Product(s):** GGSN

The following bulk statistics are new in this release:
- total-egcdr-xmit
- total-pgwcdxr-xmit
GTPP Changes in Release 15.0

GTPP Enhancements for September 30, 2013

- total-egcdr-rexmit
- total-pgwcdr-rexmit
- total-egcdr-accept
- total-pgwcdr-accept
- total-egcdr-fail
- total-pgwcdr-fail

Modified GTPP Bulk Statistics

This section identifies GTPP bulk statistics modified in release 15.0.

None for this release.

Deprecated GTPP Bulk Statistics

This section identifies deprecated GTPP bulk statistics that are no longer supported in release 15.0.

None for this release.

New GTPP Output Fields and Counters

This section identifies new GTPP show command output fields and counters available in release 15.0.

**show bulkstats variables gtp**

*Applicable Product(s): GGSN*

The following fields have been added to segregate the counters for G-CDR, e-GCDR and PGW-CDRs:

- total-egcdr-xmit
- total-pgwcdr-xmit
- total-egcdr-rexmit
- total-pgwcdr-rexmit
- total-egcdr-accept
- total-pgwcdr-accept
- total-egcdr-fail
- total-pgwcdr-fail

**show configuration, show configuration verbose, show configuration context, show configuration context verbose**

*Applicable Product(s): SGSN*

New statistics have been introduced to support LCS-MO-CDRs.

- Under GPRS Service, “lcs mo-cdr” is displayed as an accounting cdr type.
- Under SGSN Service, “lcs mo-cdr” is displayed as an accounting cdr type.
show gprs-service all

Applicable Product(s): SGSN
New statistics have been introduced to support LCS-MO-CDRs.
- Accounting cdr-types: lcs mo-cdr

show gtpp counters all

Applicable Product(s): GGSN
The following fields have been added to segregate the counters for G-CDR, e-GCDR and PGW-CDRs:
- Outstanding eGCDRs
- Possibly Duplicate Outstanding eGCDRs
- Archived eGCDRs
- eGCDRs buffered with AAAPROXY
- eGCDRs buffered with AAAMGR
- Outstanding PGWCDRs
- Possibly Duplicate Outstanding PGWCDRs
- Archived PGWCDRs
- PGWCDRs buffered with AAAPROXY
- PGWCDRs buffered with AAAMGR

show gtpp counters all

Applicable Product(s): SGSN
New statistics have been introduced to support LCS-MO-CDRs.
- Outstanding LCS-MO-CDRs
- Possibly Duplicate Outstanding LCS-MO-CDRs
- Archived LCS-MO-CDRs
- LCS-MO-CDRs buffered with AAAPROXY
- LCS-MO-CDRs buffered with AAAMGR

show gtpp counters cgf-address

Applicable Product(s): SGSN
New statistics have been introduced to support LCS-MO-CDRs.
- Outstanding LCS-MO CDRs
- Possibly Duplicate Outstanding LCSMO-CDRs

show gtpp counters group name

Applicable Product(s): SGSN
New statistics have been introduced to support LCS-MO-CDRs.

- Outstanding LCS-MO-CDRs
- Possibly Duplicate Outstanding LCS-MO-CDRs
- Archived LCS-MO-CDRs
- LCS-MO-CDRs buffered with AAAPROXY
- LCS-MO-CDRs buffered with AAAMGR

**show gtpp group**

*Applicable Product(s):* GGSN, P-GW, SAEGW, SGSN, S-GW

The following field has been added to display the status of suppression of zero volume CDRs.

- Suppress zero-volume CDRs

**show gtpp statistics**

*Applicable Product(s):* GGSN

The following fields have been added to segregate the counters for G-CDR, e-GCDR and PGW-CDRs:

- Total eGCDR transmission
- Total PGW-CDR transmission
- Total eGCDR retransmission
- Total PGW-CDR retransmission
- Total eGCDR accepted
- Total PGW-CDR accepted
- Total eGCDR transmission failures
- Total PGW-CDR transmission failures
- eGCDR transmission failure percent
- PGW-CDR transmission failure percent

**show gtpp statistics, show gtpp statistics cgf-address, show gtpp statistics debug-info, show gtpp statistics group name, show gtpp statistics verbose debug-info**

*Applicable Product(s):* SGSN

New statistics have been introduced to support LCS-MO-CDRs.

- Total LCS-MO-CDR transmission
- Total LCS-MO-CDR retransmission
- Total LCS-MO-CDR accepted
- Total LCS-MO-CDR transmission failures
- LCS-MO-CDR transmission failure percent
show gtpp storage-server statistics, show gtpp storage-server statistics verbose, show gtpp storage-server statistics group name

Applicable Product(s): SGSN
New statistics have been introduced to support LCS-MO-CDRs.
- Store Requests (LCS-MO-CDRs)
  - Sent
  - Retried
  - Success
  - Failed

show session subsystem

Applicable Product(s): GGSN
The following fields have been added to segregate the counters for G-CDR, e-GCDR and PGW-CDRs:
- Total eGCDRs
- Current eGCDRs
- Total PGW-CDRs
- Current PGW-CDRs

show session subsystem facility aaaproxy all, show session subsystem facility aaaproxy data-info, show session subsystem facility aaaproxy debug-info

Applicable Product(s): SGSN
New statistics have been introduced to support LCS-MO-CDRs.
- Total LCS-MO-CDRs
- Current LCS-MO-CDRs

show sgsn-service all

Applicable Product(s): SGSN
New statistics have been introduced to support LCS-MO-CDRs.
- Accounting cdr-types : lcs mo-cdr

Modified GTPP Output Fields and Counters

This section identifies GTPP show command output fields and counters modified in release 15.0.
None for this release.

Deprecated GTPP Output Fields and Counters

This section identifies deprecated GTPP show command output fields and counters that are no longer supported in release 15.0.
None for this release.
Chapter 9
HA Changes in Release 15.0

This chapter identifies features and functionality added to, modified for, or deprecated from 15.0 HA software releases.

**Important:** All functionality from Limited Availability Release StarOS Version 14.1 has been included in General Availability Release StarOS Version 15.0. The *Cisco ASR 5x00 Release Change Reference, Version 14.1*, details new feature descriptions and configuration, performance, and security changes for the 14.1 release.
HA Enhancements for September 30, 2013

HA Feature Changes as of September 30, 2013

This section provides information on HA feature changes in release 15.0.

Important: For more information regarding features in this section, refer to the HA Administration Guide for this release.

New HA Features

This section identifies new HA features available in release 15.0.

NEMOv4 with Multi-VRFs

The existing design of HA NEMOv4 has been extended to support multiple enterprise network being connected from one Mobile Router. A Mobile Router (MR) can be configured with devices/subnets to seamlessly access multiple enterprise VRFs, and the network traffic targeted for those different VRFs will share same MIP tunnel without compromising the privacy and security. Each VRF works independently through the MR and HA services.

This is done by separating the VRFs at the NEMO registration time, each VRF will be furnished with own set of GRE keys for the bidirectional traffic between MR and HA.

Modified HA Features

This section identifies HA features modified in release 15.0.

None for this release

HA Command Changes as of September 30, 2013

This section provides information on HA command changes in release 15.0.

None for this release.

HA Performance Indicator Changes as of September 30, 2013

This section provides information on HA performance indicator changes in release 15.0.

None for this release.
Chapter 10
HNB-GW Changes in Release 15.0

This chapter identifies features and functionality added to, modified for, or deprecated from 15.0 HNB-GW software releases.
HNB-GW Enhancements for September 30, 2013

HNB-GW Feature Changes as of September 30, 2013

This section provides information on HNB-GW feature changes in release 15.0.

Important: For more information regarding features in this section, refer to the HNB-GW Administration Guide for this release.

New HNB-GW Features

This section identifies new HNB-GW features available in release 15.0.

Femto to Femto (F2F) Handoff via CN

Previous Behavior: Prior to release 15.0, F2F Handin/Handoff was supported for Closed Mode HNBs only and was based on IMSI based lookup.

New Behavior: From release 15.0 onward, F2F Handoff has been supported for Closed, Hybrid, and Open Mode HNBs. IMSI based look-up has been replaced by target Cell-ID based look up.

Cisco HNB-GW has been enhanced to support the Femto to Femto Handoff via Core Network (CN) feature where a mobile in connected mode moves from the coverage area of one Home NodeB (HNB) to another HNB connected to the same system (ASR5K).

Earlier, the HNB-GW supported hand-in for closed mode HNBs. In such case, hand-in is allowed for an IMSI if it is the owner (i.e. it is the first IMSI in the whitelist of the HNB) of the target HNB. Also, handin is allowed if the IMSI is not the owner of the target HNB but is not present in the whitelist of any other HNB known to the HNB-GW. Now, the HNB-GW will be modified to select at target HNB using the target Cell ID information. In this case, hand-in is therefore supported for open and hybrid mode HNBs as well along with closed mode HNBs.

The HNB-GW support for the Femto to Femto Handoff via CN is in accordance with the following standards:

- 3GPP TS 23.060 Section 6.9.2.2.2: 3rd Generation Partnership Project; Technical Specification Combined Hard Handover and SRNS Relocation Procedure

Paging Optimization

The Cisco HNB-GW has been enhanced to support paging optimization such that it detects failure to page the last HNB where UE was registered and then automatically fan-out to location area (LA)/routing area (RA).

HNB-GW supports throttling of outgoing paging messages on IuH interface for closed, open, and hybrid mode HNBs. A fan-out approach has been implemented in HNB-GW such that paging messages are forwarded to a small set of HNBs, having probability of UE in its cell, detecting failed paging and then forwarding the paging message to a larger set of HNBs.

Important: It is assumed that IMSI of the UE is available in the HNB-GW if the UE has some context in HNB-GW.
Modified HNB-GW Features

This section identifies HNB-GW features modified in release 15.0.

Femto to Femto Handoff

Bulkstat variables have been added for Closed, Hybrid, and Open schemas for hnbgw-rua in order to the enhancement to add establishment cause under Connect Tx

**Previous Behavior:** Prior to release 15.0, Only RUA Connect Tx was populated when HNB-GW initiated RUA Connect towards HNB after receiving RANAP Relocation Request from Core-Node. HNB-GW did not display the RUA Connection-cause whether the RUA Connect TX cause was for a normal Call or for an Emergency Call.

**New Behavior:** Release 15.0 onwards, HNB-GW displays the RUA Connection-cause whether the RUA Connect TX cause is for a normal Call or for an Emergency Call.

HNB-GW Command Changes as of September 30, 2013

This section provides information on HNB-GW command changes in release 15.0.

**Important:** For more information regarding commands in this section, refer to the Command Line Interface Reference for this release.

New HNB-GW Commands

This section identifies new HNB-GW commands available in release 15.0.

**paging cs-domain**

The *paging cs-domain* command, with multiple keywords, has been added to define paging for the CS domain configuration in the HNB-GW service instance.

```
configure

context ctx_name

hnbgw-service hnb_svc_name

[ no ] paging cs-domain { fan-out timeout timeout_val1 | handle-unknown-imsi use-cn-paging-area | page-last-known-hnb timeout timeout_val2 }

default paging cs-domain { fan-out timeout | handle-unknown-imsi use-cn-paging-area | page-last-known-hnb timeout }

end
```

Notes:
- *hnb_svc_name* is a a previously defined HNB-GW service in the Context Configuration mode.
- *timeout_val1* sets the timeout value in seconds for the Fan-out paging configuration. It is an integer value ranging from 1 to 30. Default timeout value for CS domain is 5 seconds.
timeout_val2 sets the timeout value in seconds for paging the last known HNB. It is an integer value ranging from 1 to 30. Default timeout value for CS domain is 3 seconds.

**paging imsi-purge-timer**

The **paging imsi-purge-timer** command has been added to configure paging optimization based on the timer for purging the unregistered IMSIs for the HNB-GW service.

- **paging imsi-purge-timer timeout** timeout_val
- **default paging imsi-purge-timer timeout**

Use the following configuration example to configure paging optimization parameters based on the timer for purging the unregistered IMSIs in an HNB-GW service instance:

```
configure
  context ctx_name
    hnbgw-service hnb_svc_name
      paging imsi-purge-timer timeout timeout_val
      default paging imsi-purge-timer timeout
    end
```

**Notes:**
- timeout_val sets the timeout value for the IMSI purge timer in hours. It is an integer value ranging from 1 to 12.

**paging ps-domain**

The paging ps-domain command has been added to define paging criteria for the PS domain of the HNB-GW service.

```
configure
  context ctx_name
    hnbgw-service hnb_svc_name
      no paging ps-domain { fan-out timeout timeout_val1 | handle-unknown-imsi use-cn-paging-area | page-last-known-hnb timeout timeout_val2 }
      default paging ps-domain { fan-out timeout | handle-unknown-imsi use-cn-paging-area | page-last-known-hnb timeout }
    end
```

**Notes:**
- timeout_val1 sets the timeout value in seconds for the Fan-out paging configuration. It is an integer value ranging from 1 to 30. Default timeout value for PS domain is 10 seconds.
- timeout_val2 sets the timeout value in seconds for paging the last known HNB. It is an integer value ranging from 1 to 30. Default timeout value for PS domain is 6 seconds.
Modified HNB-GW Commands

This section identifies HNB-GW commands modified in release 15.0.
None for this release.

Deprecated HNB-GW Commands

This section identifies deprecated HNB-GW commands that are no longer supported in release 15.0.

paging open-hnb

With Paging optimization functionality in place, the following paging open-hnb commands and keywords have been deprecated in release 15.0 and onwards.

```
paging [ open-hnb { hnb-where-ue-registered fallback { always | never | only-if-with-paging-area } | always | never | only-if-with-paging-area } | hybrid-hnb { hnb-where-ue-registered { hnbs-having-imsi-in-whitelist fallback { always | never | only-if-with-paging-area } | fallback { always | never | only-if-with-paging-area } } | hnbs-having-imsi-in-whitelist fallback { always | never | only-if-with-paging-area } | always | never | only-if-with-paging-area } ]
default paging [ open-hnb | hybrid-hnb ]
```

HNB-GW Performance Indicator Changes as of September 30, 2013

This section provides information on HNB-GW performance indicator changes in release 15.0.

**Important:** For more information regarding bulk statistics and output fields and counters in this section, refer to the Statistics and Counters Reference for this release.

New HNB-GW Bulk Statistics

This section identifies new HNB-GW bulk statistics available in release 15.0.
None for this release.

Modified HNB-GW Bulk Statistics

This section identifies HNB-GW bulk statistics modified in release 15.0.
None for this release.

Deprecated HNB-GW Bulk Statistics

This section identifies HNB-GW bulk statistics modified in release 15.0.
None for this release.
New HNB-GW Output Fields and Counters

This section identifies new HNB-GW show command output fields and counters available in release 15.0.

show hnbgw-service all

The following fields/counters have been added to the Paging section of the output of above command:

- IMSI Purge Timer Value
- CS Domain: Handle unknown IMSI
- CS Domain: Page last known HNB timeout
- CS Domain: Fanout Paging timeout
- PS Domain: Handle unknown IMSI
- PS Domain: Page last known HNB timeout
- PS Domain: Fanout Paging timeout

show hnbgw statistics paging-only

Following new statistics have been added to the show hnbgw statistics command for paging-only option:

CS Domain Paging:

- Total paging RX
- Paging for unknown IMSI - Received
- Paging for unknown IMSI - Handled
- Paging for unknown IMSI - Dropped
- Paging for unknown IMSI - Success
- Paging for unknown IMSI - Failure
- Paging for last-registered-hnb - Attempted
- Paging for last-registered-hnb - Success
- Paging for last-registered-hnb - Failure
- Paging for last-registered-hnb - Skipped
- Paging for last-known-LA - Attempted
- Paging for last-known-LA - Success
- Paging for last-known-LA - Failure
- Paging for last-known-LA - Dropped

PS Domain Paging:

- Total paging RX
- Paging for unknown IMSI - Received
- Paging for unknown IMSI - Handled
- Paging for unknown IMSI - Dropped
- Paging for unknown IMSI - Success
- Paging for unknown IMSI - Failure
- Paging for last-registered-hnb - Attempted
- Paging for last-registered-hnb - Success
- Paging for last-registered-hnb - Failure
- Paging for last-registered-hnb - Skipped
- Paging for last-known-LA - Attempted
- Paging for last-known-LA - Success
- Paging for last-known-LA - Failure
- Paging for last-known-LA - Dropped

**Modified HNB-GW Output Fields and Counters**

This section identifies modified HNB-GW show command output fields and counters available in release 15.0.

None for this release.

**Deprecated HNB-GW Output Fields and Counters**

This section identifies deprecated HNB-GW output fields and counters that are no longer supported in release 15.0.

None for this release.
Chapter 11
HSGW Changes in Release 15.0

This chapter identifies features and functionality added to, modified for, or deprecated from 15.0 HSGW software releases.


Important: Correction: RoHC is not supported on the HSGW and was erroneously included in the past HSGW Administration Guide.
HSGW Enhancements for October 31, 2014

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
- NAT Enhancements
- System and Platform Enhancements

---

**CSCuq05382 - Incorrect MNC_MCC in APN of PBU**

**Feature Changes**

**Support New MCC for Three Digit MNC**

- **Previous Behavior:** For MCC 300, MNC length was derived as 2 digits.
- **New Behavior:** For MCC 300, MNC length will be derived as 3 digits.
HSGW Enhancements for June 6, 2014

CSCun42462 - HSGW CLI to allow 0 value for retries to Primary PGW

Feature Changes

HSGW CLI to allow 0 value for retries to the primary P-GW

**Previous Behavior:** Previously, the minimum number that could be configured for max-retransmissions to the primary P-GW (LMA - Local Mobility Anchor) was 1. With this value set at the minimum (1), the customer’s HSGW (MAG - Mobility Access Gateway) was forced to retry to the primary P-GW (LMA) a minimum of one more time before sending the PBU to a Secondary PGW (LMA).

**New Behavior:** Changed the CLI for the max-retransmissions num value to 0 so that the Secondary PGW (LMA) is tried after the initial Primary P-GW (LMA) PBA is not received.

Command Changes

```
max-retransmissions
```

The CLI max-retransmissions num value has been changed from 0 from 1 so that the Secondary PGW (LMA) will be tried after the initial Primary PGW (LMA) PBA is not received.

```
configure
  context context_name
    mag-service hsgw_svc_name
    max-retransmissions numcount
  end
```

Notes:

- **max-retransmissions**: The maximum number of retransmissions of Proxy MIP control messages to the LMA. `count` must be an integer from 0 through 4294967295.

CSCuo16661 - IUBE Support on HSGW

Feature Changes

Inter-User Support in HSGW
Inter-user differentiation for best effort data creates a multi-tier traffic handling differentiation among users for data applications and services. There is a customer specific request to implement Inter User differentiation for best effort data on the customer’s eHRPD network.

The 1xEV-DO Inter User QoS allows flagged users' traffic to be sent as a higher priority than non-prioritized users. This will ensure that the prioritized users are able to receive the best performance possible under the current radio frequency (RF) conditions. This prioritization becomes especially critical when the network is congested and begins dropping packets to reduce that congestion.

With 1xEV-DO Inter User QoS, network components differentiate between high-priority and low-priority users and resources are allocated to the high-priority users. At the same time, the available resources will be reduced for the lower priority users.

This is a customer specific request to control the 3GPP2-Inter-User-Priority AVP via AAA over STa during the EAP answer.

**Previous Behavior:** Previously, the customer-specific Diameter dictionary “aaa-custom9” did not have support for 3GPP2-Inter-User-Priority AVP from AAA (STa interface). This AVP was set and statically defined in the Subscriber Default configuration of the HSGW. The AVP value was configurable via CLI between 0-7.

**New Behavior:** A new Diameter dictionary “aaa-custom19” is defined to include the 3GPP2-Inter-User-Priority AVP as part of the grouped AVP “3GPP2-Information”. The 3GPP2-Inter-User-Priority AVP will be sent over STa interface in the Diameter-EAP-Answer (DEA) and AAA messages.

The HSGW uses the last 3GPP2-Inter-User-Priority values sent from AAA to provide the 3GPP2-Inter-User-Priority value to the eHRPD eRAN via A11 interface. If the 3GPP2-Inter-User-Priority AVP is missing in the DEA, then the HSGW reverts to the 3GPP2-Inter-User-Priority that was statically defined in the Subscriber Default configuration of the HSGW.

**Customer Impact:** Added the customer-specific dictionary.
HSGW Enhancements for November 30, 2013

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 & Platform Enhancements

---

**CSCuh83994 - Possible Memory Leak in sessctrl process observed in Customer CLAB setup**

**Feature Changes**

**Memory Leak in sessctrl Process Fixed**

**Previous Behavior:** There was a possible memory leak in sessctrl process observed in customer CLAB setup.

**New Behavior:** Fixed possible leaks through the following actions:

- Increased the sessctrl task memory from 67MB to 90MB.
- Made changes related to unnecessary reconciliation of APN, subscriber and imsa-service configuration.
- Removed unnecessary messaging (large number of messages) for PHSGW, PHSPC, ASNGW and ASNPC services, which are no longer supported. The messaging for these services is commented out.
HSGW Enhancements for September 30, 2013

HSGW Feature Changes as of September 30, 2013

This section provides information on HSGW feature changes in release 15.0.

**Important:** For more information regarding features in this section, refer to the *HSGW Administration Guide* for this release.

New HSGW Features

This section identifies new HSGW features available in release 15.0.

**HSGW PMIPv6 Heartbeat**

Proxy Mobile IPv6 (PMIPv6) is a network-based mobility management protocol to provide mobility without requiring the participation of the mobile node in any PMIPv6 mobility related signaling. The core functional entities Mobile Access Gateway (MAG) and the Local Mobility Anchor (LMA) set up tunnels dynamically to manage mobility for a mobile node.

Path management mechanism through Heartbeat messages between the MAG and LMA is important to know the reachability of the peers, to detect failures, quickly inform peers in the event of a recovery from node failures, and allow a peer to take appropriate action.

Per RFC 5847, PMIP heartbeats from the HSGW to the P-GW are now supported. CLI has been added to configure the heartbeat variables. Show commands have also been modified to display the heartbeat configuration and the statistics

**HSGW to Send Destination P-GW in New AVP**

The Diameter attribute “Destination-PGW” is supported.

**Important:** Note that not all attributes listed here are supported in all dictionaries. For information on attributes supported in a custom dictionary, contact your Cisco account representative. For information on attributes supported in standard dictionaries, refer to the *Diameter Attribute Quick Reference* appendix in the *AAA and GTPP Interface Administration and Reference*.

**Option to Send BSID in PBU Refresh from HSGW**

When HSGW extends the registration lifetime, the PBU (Proxy Binding Update) it sends must include the BSID (Base Station Identification). The BSID must be the last seen BSID from the RNC. The PBU sent during de-registration must also include BSID.

A new CLI has been added for mag-service to enable the user to pick and choose which PBU packets will have the BSID information and which ones will not. By default, the existing behavior of sending BSID in initialization PBU and update PBU packets will remain unchanged.

In addition, a new trigger has been added to update the BSID change information in the MAG driver for local base station migrations. For this trigger, no update PBU packet will be sent to P-GW.
Modified HSGW Features

This section identifies HSGW features modified in release 15.0.

Increase HSGW context-retention-timer Maximum

HSGW context-retention-timer timeout increased to 24 hours.

Previous Behavior: Maximum Timer value was one hour.

New Behavior: Maximum Timer value is 24 hours.

Support ‘show subs full peer-address <>’ for eHRPD Calls in HSGW

1. Added mag-address filter to the following commands:
   - show subscribers pgw-only
   - clear subscribers pgw-only

2. Added pgw-address filter to the following command:
   - show subscribers hsgw-only

3. Added hsgw-only filter to the following command:
   - clear subscribers

4. Enhanced the following existing commands to filter the pgw-address calls for all running services:
   - show subscribers pgw-address
   - clear subscribers pgw-address

HSGW Command Changes as of September 30, 2013

This section provides information on HSGW command changes in release 15.0.

Important: For more information regarding commands in this section, refer to the Command Line Interface Reference for this release.

New HSGW Commands

This section identifies new HSGW commands available in release 15.0.

heartbeat

The following command configures the PMIPv6 heartbeat message interval and retransmission timeout and max retransmission for the MAG Service.

configure

   context context_name

   mag-service svc_name
heartbeat { interval seconds | retransmission { max number | timeout seconds } }

default heartbeat { interval | retransmission { max | timeout } }

no heartbeat

end

interval: The interval in seconds at which heartbeat messages are sent from 30-3600 seconds. Default: 60 seconds.
retransmission max: The maximum number of heartbeat retransmissions allowed from 0-15. Default: 3.
retransmission timeout: The timeout in seconds for heartbeat retransmissions from 1-20 seconds. Default: 3 seconds.

**policy include-bsid-binding-update**

The following command configures the MAG Service to include BSID (Base Station Identification) in the PBU (Proxy Binding Update) sent by MAG to the P-GW. By default, BSID information is included in the update (handoff) and initialization (init) packets.

configure

    context <context_name>

    mag-service <svc_name>

        policy include-bsid-binding-update { all | none { dereg | handoff | init | renew } }

        [ default ] policy include-bsid-binding-update

    end

all: Include BSID in all the types of PBU that are sent.
none: Include BSID in none of the PBUs.
dereg: Include BSID in the PBU sent during deregistration.
handoff: Include BSID in the PBU sent during a handoff.
init: Include BSID in the PBU sent during initialization.
renew: Include BSID in the PBU sent during 'registration lifetime' renewal.

**send-destination-pgw**

The following command configures how the HSGW selects a P-GW address for the “Destination-PGW” AVP.

configure

    context <context_name>

    subscriber name <name>

        send-destination-pgw { all | explicit-only | implicit-only }

        [ no ] send-destination-pgw
end

**implicit-only**: The UE performs LCP/PPP procedures, and attaches with a specific APN. The AAA does not return the P-GW to use, so the HSGW performs NAPTR procedures to determine the P-GW which will be used.

**explicit-only**: The UE performs LCP/PPP procedures, and attaches with a specific APN. The HSGW queries the AAA over the STa interface and receives a MIP6-Agent-Info AVP that includes a sub AVP of Destination-Host. The HSGW copies the value of the Destination-Host AVP in the Destination-PGW AVP which is sent in the CCR-I to the PCRF.

all: P-GW address is obtained either by explicit or implicit mechanism.

**ue-initiated-qos**

By default, UE-initiated QoS requests are accepted and forwarded to the PCRF via Gxa interface. If PCRF rejects the UE initiated QoS, the UE request is rejected.

Issuing the `no ue-initiated-qos` command configures the HSGW to reject UE initiated QoS requests for dedicated bearer in HSGW service. The HSGW will not forward the request to the PCRF over Gxa and instead rejects the UE initiated QoS immediately.

```
configure

call-context <context_name>

  hsgw-service <svc_name>

    [ default | no ] ue-initiated-qos

end
```

**Modified HSGW Commands**

This section identifies HSGW commands modified in release 15.0.

**clear subscribers**

The `mag-address` keyword has been added to this command. This CLI command will first filter all the sessions emerging from P-GW and then further filter the ones that go to the specified MAG address. The results can be filtered further based on other options selected. Only those sessions which match the specified filters will be cleared.

```
clear subscribers pgw-only mag-address ipv4/ipv6_address [ filter_keywords ] [ verbose ] [ -noconfirm ]
```

The `hsgw-only` keyword has been added to this command. This CLI command will filter all the sessions emerging from HSGW. The results can be filtered further based on other options selected. Only those sessions which match the specified filters will be cleared.

```
clear subscribers hsgw-only [ filter_keywords ] [ verbose ] [ -noconfirm ]
```

The `pgw-address` keyword now can be used to filter for all running services. Previously this keyword was applicable only for S-GW and SAEGW services. Only those sessions which match the specified filters will be cleared.

```
clear subscribers pgw-address ipv4/ipv6_address [ filter_keywords ] [ verbose ] [ -noconfirm ]
```
context-retention-timer

The maximum value for `timeout` has been increased from 3600 seconds in previous releases to 86400 seconds (24 hours) in this release.

```
configure

    context <context_name>
    hsgw-service <svc_name>
    context-retention-timer timeout <0-86400>

end
```

The maximum value for `timeout` is 86400 seconds (24 hours).

show subscribers

The `mag-address` keyword has been added to this command. This CLI command will first filter all the sessions emerging from P-GW and then further filter the ones that go to the specified MAG address. The results can be filtered further based on other options selected.

```
show subscribers pgw-only mag-address ipv4/ipv6_address [ filter_keywords ] [ | { grep grep_options | more } ]
```

The `pgw-address` keyword has been added to this command. This CLI command will first filter all the sessions emerging from HSGW and then further filter the ones that go to the specified P-GW address. The results can be filtered further based on other options selected.

```
show subscribers hsgw-only pgw-address ipv4/ipv6_address [ filter_keywords ] [ | { grep grep_options | more } ]
```

The `pgw-address` keyword now can be used to filter for all running services. Previously this keyword was applicable only for S-GW and SAEGW services.

```
show subscribers pgw-address ipv4/ipv6_address [ filter_keywords ] [ | { grep grep_options | more } ]
```

Deprecated HSGW Commands

This section identifies deprecated HSGW commands that are no longer supported in release 15.0.

None for this release

HSGW Performance Indicator Changes as of September 30, 2013

This section provides information on HSGW performance indicator changes in release 15.0.

---

**Important:** For more information regarding bulk statistics and output fields and counters in this section, refer to the Statistics and Counters Reference for this release.
New HSGW Bulk Statistics

This section identifies new HSGW bulk statistics available in release 15.0.

New in the MAG Schema

The following bulkstats have been added:

- lma-fallback-attempted
- lma-fallback-success
- lma-fallback-failure
- lma-fallback-demux-update-fail
- lma-fallback-alt-pgw-not-found
- lma-fallback-pgw-rejects
- lma-fallback-pgw-timeouts

The following bulkstats have been added to show heartbeat statistics:

- mag-txhbreqinitial
- mag-txhbreqretrans
- mag-txhbrsptotal
- mag-rxhbreqtotal
- mag-rxhbrsptotal
- mag-rxhbrspbinderror
- mag-rxhbdiscardtotal
- mag-rxhbddecodeerror
- mag-rxhbinvalidbufflen
- mag-rxhbrspunknownpeer
- mag-rxhbrspseqnummismatch
- mag-rxhbrsprstctrmissing
- mag-pathfailurestotal
- mag-pathfailrstctrchange
- mag-pathfailnohbrsprevd

Modified HSGW Bulk Statistics

This section identifies HSGW bulk statistics modified in release 15.0.

None for this release.

Deprecated HSGW Bulk Statistics

This section identifies deprecated HSGW bulk statistics that are no longer supported in release 15.0.
None for this release.

New HSGW Output Fields and Counters

This section identifies new HSGW show command output fields and counters available in release 15.0.

show mag-service all

The following field has been added to show the configuration of the `policy include-bsid-binding-update` command:

- PBU Option

The following fields have been added to show the configuration of the `heartbeat` command:

- Heartbeat Support
- Heartbeat Interval
- Heartbeat Retransmission timeout
- Heartbeat Max Retransmissions

Modified HSGW Output Fields and Counters

This section identifies modified HSGW show command output fields and counters available in release 15.0.

show hsgw-service statistics all

Various existing fields were reorganized to make it more intuitive and informative as follows:

HSGW Node Level Statistics:

VPN Name: local

Session Level Statistics:

Total UE Statistics:

  Current UE: 0
  Setup UE: 0

PDN Statistics:

  Current PDN: 0
  Setup PDN: 0
  Released PDN: 0
  Rejected PDN: 0

Total Per-PDN Statistics:

PDN-Type IPv4 Sessions:
Active: 0  Setup: 0
Released: 0  Rejected: 0

PDN-Type IPv6 Sessions:
Active: 0  Setup: 0
Released: 0  Rejected: 0

PDN-Type IPv4v6 Sessions:
Active: 0  Setup: 0
Released: 0  Rejected: 0

Total PDNs Released Reason:
PCF Initiated: 0  PGW Initiated: 0
PCRF Initiated: 0  Local: 0
Other: 0

Total PDNs Rejected Reason:
PGW Reject: 0  APN Auth Failure: 0
PDN Already Exist: 0  Admin Prohibited: 0
No PGW Available: 0  PDN Limit Exceeded: 0
PDN GW Unreachable: 0  Resource Unavailable: 0
Subscription Limit: 0  Other: 0

**Deprecated HSGW Output Fields and Counters**

This section identifies deprecated HSGW output fields and counters that are no longer supported in release 15.0.
None for this release
HSGW Enhancements for January 31, 2014

HSGW Feature Changes as of January 31, 2014

This section provides information on HSGW feature changes in release 15.0.

**Important:** For more information regarding features in this section, refer to the *Cisco ASR 5x00 HRPD Serving Gateway Administration Guide* for this release.

**CSCuj45420 - QChat feature on HSGW**

**Feature Changes**

**Intelligent Traffic Control**

**Previous Behavior:** Previously, there was no support to load the `policy-group` defined for a subscriber for HSGW service.

**New Behavior:** The `policy-group` specified in subscriber template will be loaded and the policies specified in `policy-map` will be applicable for HSGW calls.

**Important:** Intelligent Traffic Control (ITC) includes the `class-map`, `policy-map` and `policy-group` commands. For more information on ITC, refer to the *HRPD Serving Gateway Overview and Intelligent Traffic Control* chapter in the *HRPD Serving Gateway Administration Guide*. 
Chapter 12
InTracer Changes in Release 15.0

This chapter identifies system-level features and functionality added to, modified for, or deprecated from 15.0 InTracer software releases.

**Important:** Enhancements to SNMP MIB in release 15.0 are located in the *SNMP MIB Changes* chapter.
InTracer Enhancements for January 31, 2014

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

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

**Command Changes** - changes to any of the CLI command syntax. For details, refer to the *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 InTracer.

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

---

**CSCtn31131 - Support for InTracer upgrade**

**Feature Changes**

**Support for InTracer Upgrade Added**

Method of procedure is available with current release. Intracer supports upgrade from 14.0.247 to the current version.

**Previous Behavior:** Method of procedure was not available for upgrading latest information.

**New Behavior:** Method of procedure for upgrade is supported now.
CSCua61843 - Support Required: Reset superuser password

Feature Changes

Reset Superuser Password Support Added

Support for resetting super user password is added.

Previous Behavior: There was no way to reset super user password.

New Behavior: A utility is available for resetting the password.

CSCui63599 - Display which user activated a trace

Feature Changes

Support to Display Which User has Activated a Trace

Earlier, user did not know who activated other traces. User could not know which traces were safe to be deactivated. Now, in the Active Traces screen, when you activate any trace, the user column of the table shows the user name of the user who has activated the trace. When you export the active traces to excel the username is also displayed with it.

Previous Behavior: Earlier, user did not know who activated other traces. User could not know which traces were safe to be deactivated.

New Behavior: Now, in the Active Traces screen, when you activate any trace, the user column of the table shows the user name of the user who has activated the trace. When you export the active traces to excel the username is also displayed with it.

CSCui63605 - Add auto-deactivate support for a trace

Feature Changes

Support for Auto-Deactivate for a Trace Added

Since the number of concurrent traces is limited, you can now schedule the time when the active traces needs to be deactivated. You can schedule auto-deactivate for days, hours, or minutes time. After the time is reached, the active trace gets deactivated.

Previous Behavior: There was no option to deactivate the active traces.

New Behavior: You can now schedule the time when the active traces needs to be deactivated. You can schedule auto-deactivate for days, hours, or minutes time. After the time is reached, the active trace gets deactivated.
CSCum20588 - New Disconnect reasons support

Feature Changes

Support Added for New Disconnect Reasons List

The new disconnect reasons list is reflected in the auto-generated files and on the User Interface as well.

- intra-ggsn-handoff(510)
- WSG-Auth-failed(511)
- Gtp-non-existent-pdp-context(512)
- sgsn-cancel-loc-initl-attach(513)
- Local-fallback-timeout(514)
- sgsn-nrspca-actv-rej-by-sgsn(515)
- sgsn-nrspca-actv-rej-by-ms(516)
- ims-authorization-config-delete(517)
- sgsn-no-ptmsi-signature(518)
- pgw-sel-dns-server-nt-reachable(519)
- pgw-sel-dns-no-resource-records(520)
- pgw-sel-dns-no-service-params(521)
- ePDG-Auth-failed(522)
- ePDG-pgw-sel-failure-initial(523)
- ePDG-pgw-sel-failure-handoff(524)
- sgsn-ho-sgw-reloc-collision(525)
- ePDG-dbr-from-pgw(526)
- ePDG-gtpc-abort-session(527)
- ePDG-gtpu-abort-session(528)
- ePDG-gtpu-error-ind(529)
- ePDG-pgw-not-reachable(530)
- ePDG-reject-from-pgw(531)
- IPSG-session-replacement(532)
- ePDG-release-due-to-handoff(533)
- mme-foreign-plmn-guti-rejected(534)
- sgsn-dsd-allepswithdrawn(535)
- NAT-Pool-BusyOut-Or-Pend-Delete(536)
- Invalid-APN(537)
- srvcc-ps-to-cs-handover(538)
- henbgw-mme-s1ap-reset-recd(539)
- henbgw-hnb-s1ap-reset-recd(540)
- henbgw-mme-sctp-conn-down(541)
- henbgw-hnb-sctp-conn-down(542)
- henbgw-handoff-complete(543)
- henbgw-handover-failed(544)
- henbgw-mme-error-indication(545)
- henbgw-hnb-error-indication(546)
- henbgw-hnb-initiated-release(547)
- henbgw-mme-initiated-release(548)
- henbgw-duplicate-session(549)
- Transport-mismatch-with-PGW(550)
- icsr-ipsec-chkpt-failed(551)
- sgsn-dbr-cause-isr-deact-detach(552)
InTracer Enhancements for November 30, 2013

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

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

**CSCui50281 - Random Session Trace Support in Intracer**

**Feature Changes**

**Random Trace Session**

InTracer supports random trace sessions. For this, InTracer GUI supports configuration for enabling random subscriber and also displays the trace data generated.

By default, random Trace is disabled. The user can activate the Random Trace using CLI commands or GUI.

**Command Changes**

```
session trace random
```

New CLI `session trace random` is introduced to configure the random trace with trace information. This command can be executed in Exec mode.

```
session trace random number_of_subscribers network-element {ggsn|pgw} [ interface { all | interface } ] collection-entity tce_ip_address

no session trace random network-element { ggsn | pgw }
```

Notes:

- The subscribers are selected based on the random number generated by the linear congruential algorithm.
- `number_of_subscriber` to be enabled with random trace is configured through Random trace CLI.
- Increasing the `number_of_subscriber` for random trace type is possible at any time.
- To decrease the `number_of_subscriber` in Random tracing, user has to disable and reconfigure the CLI. There is some delay between disabling and reconfiguring the Random trace activation.
InTracer Enhancements for September 30, 2013

InTracer Feature Changes as of September 30, 2013

This section provides information on InTracer feature changes in release 15.0.

**Important:** For more information regarding features in this section, refer to the *InTracer Administration Guide* for this release.

New InTracer Features

This section identifies new InTracer features available in release 15.0.

InTracer Upgrade

This feature supports upgrade to newer releases so that new functionalities are available to the end-user.

**Important:** For upgrading procedure to complete successfully, you must have already obtained the upgrade file(s) and stored them on the server running the InTracer application.

S6b Interfaces Support for Intracer

InTracer now supports S6b interface. The reference point S6b lies between the PDG (PDN Gateway) and the 3GPP AAA Proxy/Server for mobility-related authentication. This interface has the following properties:

1. Transport of commands to retrieve and store the mobility parameters.
2. Transport of static QoS.

Superuser Password Reset

This feature will allow users to reset the superuser password if forgotten.

SSL Certificates Validity Extended

The certificate validity has been increased to 3 years. It is not provided as a feature or mechanism for renewal of certificate etc. The certificate now provided will have a default validity of 3 years (as against the previous one which had only 30 days validity.)

Operator Privilege User not Allowed to view other User Traces

Administrator can create a group of operators and operators associated with this group name will only be able to see traces/data of those nodes that will be also associated with this group name.
Export of Trace details to PCAP Format

LTE Session messages can be exported to a file in ‘text/pcap’ format in your local directory. Based on the selection the processing will be done either for text export or pcap export and the relevant file will be sent back to the client for saving/downloading.

MOP for Intracer Backup and Recovery

Using this feature data can be written to the backup directory every day at 12 midnight or after 5 minutes. User has to provide the “Backup path” at the time of R-TCE and R-InTracer configuration.

Increase the number of evtproc Instances

Increase the number of evtproc instances for load sharing and to increase overall performance.

Support for Export to File feature

The search records displayed are exportable to Excel file.

Visual Call trace/call Flow

Intracer supports LTE trace sessions and displays each session details in table format on UI. Session data already available in tabular format will also be displayed in graphically format on UI. This will help user to see graphical view of call flow from one entity to other. For example from MME to SGW and vice versa.

InTracer Configuration Management Changes as of September 30, 2013

This section provides information on InTracer configuration command changes in release 15.0.

None for this release.

InTracer Performance Management Changes as of September 30, 2013

This section provides information on InTracer performance management changes in release 14.0.

Activated Traces Details included in Audit Trail

Activated trace details are included in audit trail that include:

- Trace InSync
- Trace Reference
- Subscriber Id Value
- MCC
- MNC
- Node name-type
InTracer Changes in Release 15.0

InTracer Enhancements for September 30, 2013

- Interfaces, Actions
- Trace Profile
- Subscriber Id Type

Whenever user clicks Log column from Audit logs table a dialog will be shown which will contain above activated traces details.

**Important:** For operator, Audit logs Menu will be hidden.

**Intracer Audit Logs Scheduled Purging**

This feature will enable automatic purging of audit trail logs older than a specified number of days given by the user in the Configuration page for C-Intracer. Initial default value of log storage will be 30 days. (i.e.: Audit logs will be maintained for 30 days only.)

C-Intracer will create a scheduler which will run daily to validate logs and clear them from the postgres table, if older than the specified number of days.

**Structured Archivedata Directory**

Archive directory creation is structured to make the clean up easy.

1. If the "archivedata" flag is enabled then XML parser process ("ipmsxmlparser") will create a day wise directory (YYYYMMDD) under the "archivedata" directory for storing and separating day wise XML files that are parsed.
   For example, Xmlfile: A20130213.1549+0530-PGW.GW37PGW.123456567902.6 having the date as "20130213" is taken for parsing on "20130214" then this file will be moved to the directory "20130214".

2. Cleanup script will compress all the archived XML files from the previous day directory and will store that compressed file in the "archivedata" directory. The naming convention of the compressed file will be "YYYYMMDD.tar.gz".

3. Routine cleanup activity will remove "n days" older "*.tar.gz" from the "archivedata" directory.

**Important:** Archived XML files accessibility to user: As directory creation is according to the system date so if parsing is getting delayed then some of the files can be moved to next day's directory. For example, Xmlfile: "A20130213.2359+0530-PGW.GW37PGW.123456567902.6", here the XML file's date and time is 13 Feb, 23:59 and parser has taken this file for parsing on 14 Feb, 00:20. In this case this file will be moved to "20130214" directory instead of "20130213". So with this approach, sometimes user has to open at the max 2 directories for locating archived XML file.
Chapter 13
IPSG Changes in Release 15.0

This chapter identifies features and functionality added to, modified for, or deprecated from 15.0 IPSG software releases.
IPSG Enhancements for March 31, 2014

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

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

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

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

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

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

**CSCum67780 - Gy support for IPSG to support 3GPP-RAT-Type=103 (HRPD)**

**Feature Changes**

**RAT Type HRPD mapping for IPSG**

With this release, the RAT-Type AVP for IPSG supports a new enumerated value (103) for 3GPP2 HRPD. This AVP value is encoded and sent to the Gy interface via. CCR-I messages.
IPSG Enhancements for November 30, 2013

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

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

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

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

---

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

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

---

**CSCts36707 - IPSG qualification on ASR5500 (Ares) in IPSG Server Mode**

**Feature Changes**

**IPSG Support on ASR 5500 Platform**

With this release, the ASR 5500 platform supports IPSG.

**Previous Behavior:** IPSG was supported on the ASR 5000 platform only.

**New Behavior:** The ASR 5500 platform now supports IPSG RADIUS Server configuration.
IPSG Enhancements for October 31, 2013

IPSG Feature Changes as of October 31, 2013

This section provides information on IPSG feature changes in release 15.0.

**Important:** For more information regarding features in this section, refer to the *IPSG Administration Guide* for this release.

New IPSG Features

This section identifies new IPSG features available in release 15.0.

None for this release.

Modified IPSG Features

This section identifies IPSG features modified in release 15.0.

Clear Subscriber Session based on the NAS IP Address

The support for Accounting On/Off messages for IPSG in server mode introduced in one of the earlier releases enabled IPSG to act as a Radius server. On receiving a Radius Accounting On/Off message, IPSG clears all sessions mapped to the client's L3 IP address. In certain network architectures, the L3 IP address of the Radius Accounting request message could be a Radius Proxy device located between the GGSN nodes and IPSG. This leads to IPSG terminating all the subscriber's sessions of all the APNs for GGSN.

With this release, the existing sessions are cleared based on the NAS-IP address of the subscriber that was assigned when the Acct-start message was created. If there is no NAS-IP-Address available, the peer IP address is considered as the NAS-IP-Address for the session. IPSG terminates the subscriber sessions having the same NAS-IP-Address attribute from which the Accounting On/Off message originated.

IPSG Command Changes as of October 31, 2013

This section provides information on IPSG command changes in release 15.0.

None for this release.

IPSG Performance Indicator Changes as of October 31, 2013

This section provides information on IPSG performance indicator changes in release 15.0.

None for this release.
IPSG Enhancements for September 30, 2013

IPSG Feature Changes as of September 30, 2013

This section provides information on IPSG feature changes in release 15.0.

Important: For more information regarding features in this section, refer to the IPSG Administration Guide for this release.

New IPSG Features

This section identifies new IPSG features available in release 15.0.

Lawful Intercept Support for IPSG

The Lawful Intercept feature is now supported on IPSG. For more information, contact your Cisco representative.

Support for Peer Selection at Diabase

In the earlier Gx implementation, Diameter Policy Control Application has the limitation to mandatorily configure hosts as part of IMS Authorization service or associate a host template and select the hosts to be communicated for each subscriber session. Since the peer selection can occur at diabase, and the application need not select any hosts, this feature is introduced to remove the restrictions imposed in the application and allow diabase to pick the peers in a round-robin fashion. In addition, this feature addresses peer selection at diabase even when the hosts picked by application are not active. This change in behavior is controlled through the CLI command endpoint-peer-select as the default behavior is to drop the call if the server discovery fails at application.

When the peers are selected from endpoint, the output of CLI command show ims-authorization sessions full does not display the "Primary PCRF Server" and "Secondary PCRF Server" fields.

CC-Time AVP in Gx for IPSG

IPSG now supports the CC-Time AVP to be parsed in the Granted Service Unit (GSU) message sent over Gx interface. This AVP support is required for time reporting based billing to subscribers. For more information on the Time Reporting over Gx (TRoGx) feature, see the Gx Interface Support appendix of the IPSG Administration Guide.

Support for VLANS and Overlapping IP Addresses

Important: This is a customer-specific feature. For more information, please contact your Cisco account representative.

This release introduces support for overlapping IP addresses for subscribers serviced by access networks on IPSG using VLAN on the Sn interface.

Overlapping IP addresses can be set up by defining multiple interfaces on the Sn side and binding them to separate VLANs, while a single interface is setup to separate traffic using VPNv4 on the Si side. When IPSG receives a packet,
the appropriate session is identified based on the combination of IP address and VLAN. This feature currently supports configuration to a maximum of 500 VLANs.

**Validate RADIUS Client IP**

This feature enables the ipsgmgr to validate RADIUS accounting messages from different configured RADIUS client IP address, and forward requests to the session manager. The client IPs are validated by default and can be disabled using the CLI command.

**Modified IPSG Features**

This section identifies IPSG features modified in release 15.0.

None for this release.

**IPSG Command Changes as of September 30, 2013**

This section provides information on IPSG command changes in release 15.0.

---

**Important:** For more information regarding commands in this section, refer to the *Command Line Interface Reference* for this release.

---

**New IPSG Commands**

This section identifies new IPSG commands available in release 15.0.

**overlapping-ip-address**

This command allows you to enable or disable overlapping of IP addresses which enables multiple users to use the same IP address.

```config
  context context_name

  ipsg-service service_name mode radius-server

  { default | no } overlapping-ip-address

end
```

**endpoint-peer-select**

This command is used to perform server selection at Diabase when the hosts could not be selected by application or when the hosts selected by the IMS Authorization application is inactive. For example, host table is not configured in IMSA service, host table is configured but not activated, none of the rows in prefix table match the subscriber, host template is not associated with IMSA service, host template could not select the hosts.

```config
  context context_name
```

---

Cisco ASR 5x00 Release Change Reference
**Modified IPSG Commands**

This section identifies IPSG commands modified in release 15.0.

**sess-replacement**

This command allows you to enable/disable the Session Replacement feature for eWAG and IPSG services.

With this release, the `with-diff-acct-sess-id` keyword can be used in combination with the `with-diff-key` keyword to enable replacement options of different key and different account session ID.

```
config

       context context_name

       ipsg-service service_name mode radius-server

       sess-replacement with-diff-key [ with-diff-acct-sess-id ]

       end
```

**host-select row-precedence**

The existing CLI command in the Diameter Host Template Configuration mode is modified to enable the selection of Diameter peer based on the configured prefix/suffix/range values of IMSI or MSISDN of subscriber. This configuration change allows the overlapping range of IMSI or MSISDN values. PCRF peer selection is based on the first match of prefix/suffix/range on row precedence priorities.

With this feature being turned on, the primary and the secondary hosts configured can be picked up in an active standby mode or in round robin fashion.

```
config

       diameter-host-template template_name

       host-select row-precedence precedence table { { range-table { 1 | 2 } { imsi-based { [ prefix | suffix ] imsi-value [ to imsi-value ] } | msisdn-based { [ prefix | suffix ] msisdn-value [ to msisdn-value ] } } host host_name [ realm realm_id ] [ secondary host sec_host_name realm sec_realm_id ] algorithm { active-standby | round-robin } ] } [ -noconfirm ]

       no host-select row-precedence precedence table { 1 | 2 | range-table { 1 | 2 } } [ -noconfirm ]

       end
```
host-select row-precedence

The existing CLI command in the Diameter Host Template Configuration mode is modified to enable the selection of Diameter peer based on the configured prefix/suffix/range values of IMSI or MSISDN of subscriber.

Configuring this command enables activating the configured IMSI or MSISDN table for peer selection.

```
config
diameter-host-template template_name
  host-select table { 1 | 2 | range-table { 1 | 2 } } algorithm { ip-address-modulus [ prefer-ipv4 | prefer-ipv6 ] | msisdn-modulus | round-robin } 
  no host-select table
end
```

radius accounting

This command allows you to specify the IP address and shared secret of the RADIUS accounting client from which RADIUS accounting requests are received. The RADIUS client can be either the access gateway or the RADIUS accounting server depending on which device is sending accounting requests.

With this release, the `validate-client-ip` keyword is introduced to enable the ipsgmgr to validate RADIUS accounting messages from different configured RADIUS client IP address, and forward requests to the session manager.

```
config
  context context_name
  ipsg-service service_name mode radius-server
    [ default | no ] radius accounting validate-client-ip
end
```

Default: The RADIUS client IPs are validated.

Deprecated IPSG Commands

This section identifies deprecated IPSG commands that are no longer supported in release 15.0.

None for this release.

IPSG Performance Indicator Changes as of September 30, 2013

This section provides information on IPSG performance indicator changes in release 15.0.

Important: For more information regarding bulk statistics and output fields and counters in this section, refer to the Statistics and Counters Reference for this release.
New IPSG Bulk Statistics

This section identifies new IPSG bulk statistics available in release 15.0.

None for this release.

Modified IPSG Bulk Statistics

This section identifies IPSG bulk statistics modified in release 15.0.

None for this release.

Deprecated IPSG Bulk Statistics

This section identifies deprecated IPSG bulk statistics that are no longer supported in release 15.0.

None for this release.

New IPSG Output Fields and Counters

This section identifies new IPSG show command output fields and counters available in release 15.0.

**show ipsg service**

This command displays information about the configured IPSG services.

With this release, the following field has been added to the *show ipsg service [ name service_name | all ]* command to display whether the overlapping IP address is enabled or disabled:

- Overlapping IP address

**show ipsg sessions**

This command displays information about the configured IPSG sessions.

With this release, the following field has been added to the output of the *show ipsg sessions [ full ] [ all ]* command.

- VLAN ID

**show subscribers full all**

This command displays subscriber information.

With this release, the following field has been added to the output of the *show subscribers [ full ] [ all ]* command.

- vlan id

Modified IPSG Output Fields and Counters

This section identifies modified IPSG show command output fields and counters available in release 15.0.

None for this release.
Deprecated IPSG Output Fields and Counters

This section identifies deprecated IPSG output fields and counters that are no longer supported in release 15.0.

None for this release.
Chapter 14
MME Changes in Release 15.0

This chapter identifies features and functionality added to, modified for, or deprecated from 15.0 MME software releases.

The following points to changes made in this document to correct omissions or technical errors made in the previously published Release Change Reference. In content for:

- June 6, 2014:
  - Added “CSCts21153 - Change bulkstats variable for Retransmitted SCTP data chunks”
MME Enhancements for 15.0 MR6

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

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

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

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

---

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

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

---

CSCuq88194 - New Reject cause needs to be added under Bearer Alloc Reject ESM message

**Feature Changes**

**Counter and Stats Added to Track Reject Cause**

**Previous Behavior:** The “EPS QoS Not Accepted” reject cause was not available for use in Bearer Alloc Reject ESM control messages.

**New Behavior:** The “EPS QoS Not Accepted” reject cause code is now supported for use in the Bearer Alloc Reject ESM control message. This cause code is received when UE-initiated dedicated bearer request is rejected by the MME as a result of the MME’s configuration settings in the APN Profile - 'reject’ option set with the `dedicated-bearers { gbr | non-gbr }` command.

Corresponding counter and bulk statistic variable have been added to track the use of this cause code.
Customer Impact: Support for this cause code will assist customers to debug the reject cause for bearer allocation failures.

Performance Indicator Changes

MME Schema

Use of the “EPS QoS Not Accepted” reject cause code for bearer allocation failures, is tracked as a bulk statistic in the MME schema:

- esm-msgtx-brralloc-rej-eps-qos-not-accepted

show mme-service statistics

Use of the “EPS QoS Not Accepted” reject cause code for bearer allocation failures, is tracked with the following new output counter generated by the show mme-service statistics command:

- EPS QoS Not Accepted

CSCur13994, CSCur89572 - ’State/Location Information Retrieval’ flag support in Feature-list AVP

Feature Changes

State/Location Information Retrieval’ Flag

With this release, the MME now sends the “State/Location-Information-Retrieval” flag set in the Feature-List AVP of the Update Location Request (ULR) message over the S6a interface to the HSS at the time the UE attaches. With the “State/Location-Information-Retrieval” flag set, the HSS knows to set the “EPS User State Request”, “EPS Location Information Request” and “Current Location Request” bits in the IDR-Flags AVP in IDR messages towards the MME. This subscriber data provides the UE’s current location information needed in multiple service scenarios, such as VoLTE services on the IMS side.

MME behavior for IDR-initiated Paging: Upon receipt of an IDR message with the “Current Location Request” bit set in the IDR-Flags AVP, the MME behavior complies with Feature-List AVP, IDR-Flags AVP, and EPS-Location-Information AVP sections as specified in 3GPP TS 29.272 v11.9.0. So when the IDR messages are received with “EPS Location Information Request” and “Current Location Request” bits set in IDR-Flags AVP, the MME sends the UE’s current location information or the UE’s last known location information in the “EPS-Location-Information” AVP of the IDA message.

If IDR is received with “EPS Location Information Request” and “Current Location Request” flags set in IDR-Flags AVP, the the MME’s IDA response depends on whether:

- the UE is in connected mode with Location Reporting active making location information available, then the MME sends the IDA message without “Current-Location-Retrieved” AVP in “EPS-Location-Information” AVP.
- the UE is in connected mode without Location Reporting active so location information is not available, then the MME sends a Location-Reporting-Control message to the eNB to get the ECGI and the TAI.
- If the MME receives a Location-Report message, then the MME sends an IDA message without "Current-Location-Retrieved" AVP and the "Age-Of-Location-Information" is set to zero in the "EPS-Location-Information" AVP sent to the HSS.
- If the MME does not receive a Location-Report message, then the MME sends IDA message with last known location information with "Age-Of-Location-Information" AVP and without "Current-Location-Retrieved" AVP to the HSS.

- the UE is in idle mode, then the MME pages the UE to bring the UE to connected mode.
  - If paging is successful, then the MME sends an IDA message with "Age-Of-Location-Information" and "Current-Location-Retrieved" both set to zero in the "EPS-Location-Information" AVP to the HSS.
  - If paging is not successful, then the MME sends IDA messages with last known location information with "Age-Of-Location-Information" AVP and without "Current-Location-Retrieved" AVP to the HSS.

**Location Reporting Control** messages allow the MME to request the eNB to report where the UE is currently located.

**MME’s IDR-initiated Paging Process:** If the UE is in ECM-IDLE and the MME receives IDR with "EPS Location Information Request" and "Current Location Request" flags set in IDR-Flags AVP, then the MME starts a timer for 25 seconds and triggers the paging procedure. If the MME receives a response from the eNB before the timer expires, then MME sends an IDA message with the UE’s current location information in the "EPS-Location-Information" AVP.
Otherwise the MME sends an IDA message with the last known location information in "EPS-Location-Information" AVP when the IDR timer expires.

Paging initiation is similar to paging for signaling events. However, a separate event shall be used in this case and be processed. If the paging procedure is already running for that UE, then when IDR is received with both flags set the MME shall not trigger paging again. MME behavior depends on the precedence configuration under paging-map:

- If the paging procedure already running for the UE has a higher precedence than for IDR, then when IDR is received with both flags set and if the other paging is not successful, then the MME does not trigger IDR paging again.
- If the paging procedure already running for the UE has a lower precedence than for IDR, and if IDR is received with both flags set, then the MME stops the ongoing paging procedure and triggers an IDR paging procedure.

If the paging procedure completes before the IDR timer expires and a paging response is not received from the eNB, then the MME sends an asynchronous IDA response immediately without waiting for IDR timeout.

**Command Changes**

**precedence**

A new option, `idr`, has been added as a paging trigger option to the signaling filter of the traffic-type keyword of the `precedence` command. The `precedence` command `precedence` enables the operator to apply a priority for different paging-profiles based on traffic type. When the MME service is associated with a paging map, the system checks the profile map to determine which paging-profile to adopt for a given paging trigger, such as an IDR.

**Important:** If precedence is not configured, then the lowest precedence is automatically assigned.

```
configure
lte-policy

    paging-map paging_map_name
```
precedence precedence traffic-type signaling [ idr ] paging-profile
paging_profile_name

no precedence precedence
end

Notes:
- no precedence precedence removes the precedence configuration associated with the specified precedence value.
- paging_map_name must be an alphanumeric string of up to 64 characters to identify a unique paging map associated with the LTE Policy.
- precedence must be an integer from 1 (highest precedence) to 4 (lowest precedence) to specify the handling precedence for this particular configuration definition.
- idr option selects IDR as the signaling traffic sub-type that triggers paging.
- paging_profile_name must be an alphanumeric string of up to 64 characters to identify a unique paging profile associated with the paging map and the LTE Policy.

Performance Indicator Changes

MME Schema

The following bulk statistics have been added to the MME schema to track paging initiated in response to IDR:
- signaling-idr-paging-init-events-attempted
- signaling-idr-paging-init-events-success
- signaling-idr-paging-init-events-failures
- signaling-idr-paging-last-enb-success
- signaling-idr-paging-last-tai-success
- signaling-idr-paging-tai-list-success

show mme-service statistics

New counters have been added, to the output generated by this command, to display quantitative data for successes and failures of paging initiated in response to IDR:

Paging Initiation for SIGNALING IDR Events:

Attempted: 0 Success: 0

Failures: 0

Success at Last n eNB: 0 Success at Last TAI: 0

Success at TAI List: 0

show lte-policy paging-map
The `show lte-policy paging-map name map_name` command allows you to see the precedence information configured, for example:

```
asr5000# show lte-policy paging-map name pml

=====================================================================
Paging Map : pml
=====================================================================

Precedence 1 : Signaling-IDR ; Paging is performed as per paging-profile ppl
```

**show hss-peer-service statistics**

In support of the new 'State/Location Information Retrieval' flag functionality, new counters have been added to the output generated by the `show hss-peer-service statistics` command:

- Asynchronous Message Stats:
- Asynchronous ISDR Req
- Asynchronous ISDA
- Asynchronous ISDA Dropped

**CSCur27407 - NewConnectionsNotAllowed SNMP trap firing a lot**

**Feature Changes**

**Processing SessMgr Location**

**Previous Behavior:** When the SessMgr Location procedure failed during the MME's processing of a received request (Attach / TAU request with FGUTI, GTPv2 Forward Relocation request, and GTPv1 Forward Relocation request), then the MME rejects the request and sends a trap "MMENewConnectionsNotAllowed" with reason "location of sessmgr resource failed".

**New Behavior:** If the SessMgr Location procedure fails during the MME's processing of a received request (Attach / TAU request with FGUTI, GTPv2 Forward Relocation request, and GTPv1 Forward Relocation request), then a new SessMgr is allocated, the request is processed, and the MME does not send the trap "MMENewConnectionsNotAllowed" with reason "location of sessmgr resource failed".

**Customer Impact:** Fewer requests rejected.
CSCur38243 - MME discards EGTP_CREATE_INDIRECT_DATA_FORWARDING_TUNNEL_RSP

Feature Changes

Extended Validation Options for UL F-TEID during HO

Up Link - Fully qualified Tunnel End Point Identifier

Previous Behavior:
- The MME did not accept ‘up link fully qualified tunnel end point identifier’ (UL F-TEID) in a Create Indirect Data Forwarding Response and response was dropped).
- The MME would only accept a UL F-TEID in a Create Indirect Data Forwarding Response from the S-GW if the IE instance was 4 and the interface type was set at 28 (SGW GTP-U interface for UL data forwarding).

New Behavior: The validation process has been modified so that the MME now accepts UL F-TEID in a Create Indirect Data Forwarding Response during intra-EUTRAN handover. So, the MME does not drop the response if the IE of the UL F-TEID instance is 4 and the interface type is set to either 28 (SGW GTP-U interface for UL data forwarding) or 1 (S1-U SGW GTP-U interface).

Customer Impact: The MME will accept a broader range of responses from the S-GW.

CSCur50736 - PDN Connectivity Reject : Incorrect ESM cause#27

Feature Changes

Configuring ESM Cause Code #27

In general, much of the UE behavior depends on factory configuration; for example, some operator-tied phones consider APN subscriptions as RAT specific. But many operators have configured APN as RAT agnostic. This behavior changes allows some operator flexibility to handle either type of UE configuration.

Previous Behavior: By default, the MME sent cause code value #27 (Unknown or Missing APN) in standalone PDN Connectivity Reject messages when the UE requested APN was not subscribed for that subscriber.

New Behavior: As part of the MME’s local cause code mapping, a new cause code option can be configured - "Requested-Option-Not-Subscribed" cause code value #33. When the new option is configured, then the MME sends cause code #33 (Requested Service Option Not Subscribed) in the standalone PDN Connectivity Reject message whenever the UE-requested APN is not subscribed. If the option is not configured, then by default the MME uses the cause code value #27 (Unknown or Missing APN) in standalone PDN Connectivity Reject message when the UE-requested APN is not subscribed.

Command Changes

local-cause-code-mapping

The new keyword apn-not-subscribed is added to specify the local cause-code mapping when the UE-requested APN is not subscribed for that subscriber. If cause code mapping for apn-not-subscribed is explicitly configured with requested-service-option-not-subscribed in either the Call-Control-Profile or MME-Service configuration mode,
then the new code "Requested-Option-Not-Subscribed" (cause-code #33) will be sent in the Reject message when the PDN Connectivity Request is rejected because no subscription is found.

```
configure

   call-control-profile profile_name

       local-cause-code-mapping { apn-not-subscribed esm-cause-code requested-service-option-not-subscribed }

       remove local-cause-code-mapping apn-not-subscribed

   end

Notes:

- remove - deletes the local cause code mapping from the configuration.

local-cause-code-mapping

The new keyword `apn-not-subscribed` is added to specify the local cause-code mapping when the UE-requested APN is not subscribed for that subscriber. If cause code mapping for `apn-not-subscribed` is explicitly configured with requested-service-option-not-subscribed in either the Call-Control-Profile or MME-Service configuration mode, then the new code "Requested-Option-Not-Subscribed" (cause-code #33) is sent in the Reject message when the PDN Connectivity Request is rejected because no subscription is found.

```
configure

   context context_name

       mme-service service_name

           local-cause-code-mapping { apn-not-subscribed esm-cause-code requested-service-option-not-subscribed }

           default local-cause-code-mapping apn-not-subscribed

   end

Notes:

- default - returns the local cause code mapping to the default of #27 (Unknown or Missing APN).

**Important:** `service_name` must be unique across all contexts.

- default - returns the local cause code mapping to the default of #27 (Unknown or Missing APN).

Performance Indicator Changes

**show call-control-profile full name**

A new field has been added to the output of this command to indicate the operators Call-Control-Profile configuration for this cause code mapping:

- APN not subscribed : Requested service option not subscribed
show configuration

A new field has been added to the MME-Service output section of this command to indicate the operators MME-Service configuration for this cause code mapping:

- local-cause-code-mapping apn-not-subscribed esm-cause requested-service-option-not-subscribed

show mme-service name

A new field has been added to the output of this command to indicate the operators MME-Service configuration for this cause code mapping:

- APN not subscribed : Requested service option not subscribed

CSCur89996 - MME releases UE context with Category NAS : Unspecified for Radio issues

Feature Changes

Configuring the Cause Code Mapping for UE-CONTEXT-RELEASE Sent from MME

Previous Behavior: By default, when a UE was in connected state with an MME and whenever the MME received a TAU Request over Initial-UE, then the MME initiated a UE-CONTEXT-RELEASE with cause NAS-Unspecified.

New Behavior: Now, by default, an MME initiates the UE-CONTEXT-RELEASE with cause NAS-Normal-Release whenever the MME receives a TAU Request over Initial-UE if the UE is in the connected state. As well, the CLI has been changed to enable the operator to configure a preferred cause code for init-ue-from-enodeb-for-tau.

Customer Impact: This change only impacts a customer if the customer update their KPI calculation based on this cause.

Command Changes

s1-ue-context-release

This new CLI command enables the operator to specify the cause code to be sent in UE-CONTEXT-RELEASE initiated by the MME upon the reception of TAU Request over INITIAL-UE message when a UE is in connected state.

configure

context context_name

mme-service service_name

s1-ue-context-release reason init-ue-from-enodeb-for-tau cause type { nas value nas_value | radio value radio_value }

default s1-ue-context-release reason init-ue-from-enodeb-for-tau cause

end
Notes:

**Important:** *service_name* must be unique across all contexts.

- This CLI enables the operator to configure the MME cause code mapping to be sent in a UE-CONTEXT-RELEASE message initiated from MME due to the reception of TAU procedure on Initial-UE message from the same eNB or from a different eNB. The configured cause code will be sent in the UE-CONTEXT-RELEASE message whenever MME releases the existing S1AP connection upon receiving a TAU procedure in an Initial-UE message.
- Currently, the only release reason possible is ‘init-ue-from-enodeb-for-tau’.
- There are two cause options for which cause code values can be assigned:
  - **nas value** *nas_value* options are:
    - 0 - Normal Release (default value)
    - 1 - Authentication Failure
    - 2 - Detach
    - 3 - Unspecified
    - 4 - CSG Subscription Expiry
  - **radio value** *radio_value* must be an integer from 0 to 38.

**CSCur97956, CSCun97512 - Enabling Paging Optimization**

**Feature Changes**

**Enabling Paging Optimization**

**Previous Behavior:** The MME’s paging cache functionality was disabled.

**New Behavior:** It is now possible for the operator to use CLI commands to enable and control the MME’s paging cache functionality.

**Command Changes**

**mme paging cache**

The new **mme paging cache** keyword ranges for this command, in the LTE Policy configuration mode, enable the operator to more easily enable or disable caching of the MME’s paging.

```plaintext
configure
  lte-policy
    mme paging cache { size cache_size | timeout time }
    default mme paging cache { size | timeout }
```
Notes:

- **size cache_size**: Enter an integer from 0 to 10000 to specify the maximum number of tracking area code (TAC) entries to be cached. Entering the ‘0’ value disables caching and should be followed by use of the `mme paging cache clear` command (see CSCus14148).

- **timeout time**: Enter an integer from 1 to 1440 to specify the number of minutes that each TAC entry remains valid. A lower cache timeout helps to refresh the cache frequently and enables this functionality to quickly adapt to changes in the network. We recommend the `timeout` value be less than the expected eNodeB flap frequency; for example, if the eNodeBs connected to the MME are expected to disconnect and reconnect every 10 minutes (due to network issues), then the timeout configuration should be less than 10 minutes.

- Defaults: cache size = 5000 TAC entries per SessMgr; timeout time = 5 minutes.

- Both size and timeout must be configured to enable paging caching optimization.

CSCus00927 - S1 and SGs associations not equally distributed across mmemgr tasks

Feature Changes

Configuring the MMEDEMUX

**Previous Behavior**: MMEDEMUX had insufficient waiting time to distribute the incoming traffic to the associated MMEMGRs because all MMEMGRs were not up and running on startup of the box.

**New Behavior**: A new CLI command is introduced in the MMEDEMUX system, which allows operators to configure the percentage of MMEMGRs to be associated, and the waiting time to process the incoming traffic. The MMEDEMUX distributes the incoming traffic to the associated MMEMGRs based on the percentage value and wait time configured in this command.

**Customer Impact**: The new configuration provides the following:

- By default, MME waits for ten minutes to check if 90% of the MMEMGRs have started.
- MMEDEMUX allows users to configure the waiting time up to 3600 seconds.
- MMEDEMUX allows users to configure from 1 to 100% of the available MMEMGRs.

Command Changes

**task facility mmedemux**

The new CLI command `mmedemux` allows users to configure the waiting time of the MMEDEMUX and the percentage of MMEMGRs associated with the MMEDEMUX.

```
configure

    task facility mmedemux mmemgr-startup-percentage percent_value [ mmemgr-startup-wait-time wait_time ]
```
[ default | no ] task facility mmedemux mmemgr-startup-percentage mmemgr-startup-wait-time
end

Notes:
- `mmemgr-startup-percentage` allows users to configure the percentage of MMEMGRs to be associated with the MMEDEMUX
- `percent_value` an integer from 1 to 100
- `mmemgr-startup-wait-time` allows users to configure the waiting time of MMEDEMUX
- `wait_time` an integer value from 300 to 3600
- `[ default | no ]` disables user defined configuration and replaces the configuration with default configuration values.

Performance Indicator Changes

show configuration

If the mmedemux command is used to configure the percentage of MME Managers and wait time of the MME Demux, the following configuration is displayed on executing the command `show configuration`

- task facility mmedemux mmemgr-startup-percentage mmemgr-startup-wait-time

show session subsystem facility mmedemux all

The following new statistics are displayed on executing the command `show session subsystem facility mmedemux all`:

- MMEDemux MMEMGR Startup Status
- Max MME Managers
- Desired MME Managers
- Current MME Managers
- MMEMGRs Start in Progress
- Time Left
- All Required MMEMGRs are UP
- Time taken

Notes:
The following are status indicators
- MMEMGRs Start in Progress
- Time Left
- All Required MMEMGRs are UP
- Time taken
CSCus14148 - Dynamic Paging cache size allocation through CLI

Feature Changes

Configuring Paging Cache Functionality

**Previous Behavior:** The MME’s paging cache size could be configured to vary from 100 to 10000 tracking area code (TAC) entries.

**New Behavior:** The MME now supports an enhanced range for configuring the size of the paging cache. The configurable range has been expanded to 0 to 10000 TAC entries. Entering the ‘0’ value disables caching and should be followed by use of the `mme paging cache clear` command.

**Customer Impact:** Change ensures increased flexibility for operator to disable and/or control paging cache functionality

Command Changes

```plaintext
mme paging cache

The new configurable values range for the `mme paging cache` command enables the operator to more easily enable or disable caching of the MME’s paging.

```configure
lte-policy

mme paging cache { size cache_size | timeout time }

default mme paging cache { size | timeout }

declare
end

Notes:
- **size cache_size:** Enter an integer from 0 to 10000 to specify the maximum number of TAC entries to be cached. Entering the ‘0’ value disables caching and should be followed by use of the `mme paging cache clear` command.

mme paging cache clear

The new `mme paging cache clear` command, under the Exec mode, enables the operator to clear the paging cache for either a specific SessMgr or for all SessMgs:

```plaintext
mme paging cache clear { all | instance sessmgr_instance }

Notes:
- **all:** Instructs the MME to clear the paging cache for all Session Managers.
- **instance sessmgr_instance:** Enter an integer from 0 to 4294967295 to specify a single Session Manager.

show lte-policy
A new filter, **paging cache parameters**, has been added to the **mme** keyword in this command to display the current configuration cache parameters.

```bash
show lte-policy mme paging cache parameters
```

The command generates a display similar to the following:

```
[local]MME1# show lte-policy mme paging cache parameters
MME Paging Cache Timeout: 5
MME Paging Cache Size: 5000
```

**CSCus25950 - [VoLTE] After IDR of T-ADS for Volte, MME modifies QoS of APN**

**Feature Changes**

**Changes in Handling of Standalone ISDR from HSS**

**Previous Behavior:** Comparing negotiated QoS and subscription QoS caused the MME to trigger the Modify Bearer Command (MBC) when standalone ISDR was received from the HSS without subscription data.

**New Behavior:** Comparing negotiated QoS and subscription QoS no longer causes the MME to trigger the Modify Bearer Command (MBC) when standalone ISDR is received from the HSS without subscription data. (Main AVP subscription-data is a mandatory IE. But when it has no further sub-IEs, such as APN-configuration-profile, then MBC is not sent.)

**Customer Impact:** Signaling reduced for standalone ISDR handling when it is received without subscription data.

**CSCus50162 - QOS : Incorrect Reliability Class Mapping from QCI=5**

**Feature Changes**

**Improve Reliability Class Mapping**

During handovers involving Inter-RAT, some UEs experienced issues with existing behavior, which required the UEs to be powered off/on (reboot) to acquire service. Those issues should be resolved with the behavior changes identified below.

**Previous Behavior:** In situations where the SDU error ratio = 10*-6, the MME and SGSN each implemented QoS mapping of reliability class =2.

**New Behavior:** The MME and SGSN behavior has been modified such that in situations where the SDU error ratio = 10*-6, the MME and SGSN each implement QoS mapping of reliability class =3.
MME Enhancements for October 31, 2014

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

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

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

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

---

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

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

---

**CSCui42276 - CxGW - ‘show subscribers sgw-address <IP>’ not working as expected**

**Command Changes**

```plaintext
show subscribers sgw-address
```

The `sgw-address` keyword was previously visible on other nodes without an MME license installed, even though it was applicable only to the MME. In this release, this keyword is now visible only on StarOS systems which have a valid MME license installed.

```plaintext
show subscribers sgw-address ip_address
```
CSCui64993 - MME - call-control-profile qos ue-ambr prefer-as-cap problems

Feature Changes

QoS Cap Preference for APN-AMBR

**Previous Behavior:** The MME was not checking the QoS capping preference for the APN-AMBR if the preferred capping type was set to Local and minimum of HSS and Local.

Also, the output of the `show apn-profile full name` and `show call-control-profile full name` commands did not display the proper values for the configured QoS capping preference for APN-AMBR and UE-AMBR.

**New Behavior:** The MME now checks the configured QoS capping preference while validating the APN-AMBR values with the subscription information received from HSS.

The output of the `show apn-profile full name` and `show call-control-profile full name` commands now display the proper values for the configured QoS capping preference for APN-AMBR and UE-AMBR.

CSCuo17932 - MME sending old QoS values to UE after HO from 2G>4G>2G

Feature Changes

External Messaging Behavior Change

**Previous Behavior:** When a subscriber comes to the MME from SGSN, the MME was always sending 4G Native QOS in GMM QOS IE in NAS messages, and re-sending the obsolete QOS value received by SGSN earlier to SGSN in case of a subsequent handoff to GN/GP SGSN.

**New Behavior:** A new command is provided which controls which QOS the MME uses in NAS GMM QOS IE and GTPV1 Context response messages during a handover or inter-rat TAU with a GN/GP SGSN.

The MME can either send the QOS sent from peer SGSN, or the native EPS (4G) QOS value received from HSS. The default behavior is to send the native EPS (4G) QOS to the SGSN.

Command Changes

```
nas gmm-qos-ie-mapping
```

This new command controls which QOS the MME uses in NAS GMM QOS IE and GTPV1 Context response message during a handover or inter-rat TAU with a GN/GP SGSN.

```
context context_name

mme-service <mme_svc_name>

nas gmm-qos-ie-mapping { native-eps-qos | gngp-imported-qos }

[ default ] nas gmm-qos-ie-mapping
```
Notes:
  - The default behavior is to use the native EPS QoS.

Performance Indicator Changes

show mme-service all

The `show mme-service all` command now displays the configuration of this command in the following field:
  - NAS GMM QOS Mapped From

CSCuo27283 - Roaming QoS Control

Feature Changes

Roaming QoS Control

Previous Behavior: When the `qos prefer-as-cap both-hss-and-local minimum` configuration is set in APN Profile, the MME sends minimum values of only APN-AMBR and sends HSS values of QCI and ARP to S-GW. The expected behavior should have been to have the minimum values sent for QCI, ARP and APN-AMBR for a roaming session.

The MME also did not have the ability to configure whether to accept/reject GBR and Non-GBR dedicated bearers.

New Behavior: 1. The functionality of the APN Profile mode command `qos prefer-as-cap both-hss-and-local minimum` is now extended to QCI and ARP in APN profile for roamers. This S6A control is applied whenever the MME needs to apply Subscribed QoS. The relevant procedures are Create Session Request (Attach, UE requested PDN connectivity) and Modify Bearer Command (ISD from HSS).

The MME takes into account the HSS-Provided and Locally-Configured QoS parameters and the minimum of QCI, APN-AMBR, ARP, ARP-PCI and ARP-PVI will be sent in the Create Session Request. Note: This enhancement is supported only for Default bearers (i.e Non-GBR bearers) in a roaming scenario.

2. A new CLI is added in the APN Profile mode to provide configurability at MME to accept, reject, or locally-cap P-GW upgraded QoS values for default (non-GBR) bearers. This S11 Control is applied whenever QoS parameters are received on S11 interface. The relevant procedures for default bearers are Create Session Response (sent by P-GW during Attach, UE requested PDN connectivity) and Update Bearer Procedures (initiated by P-GW resulting from trigger QoS change or other in PCEF/PCRF, or from Modify Bearer Command or Bearer Resource Command sent by MME). Note: This enhancement is supported only for Default bearers (i.e Non-GBR bearers) in a roaming scenario.

3. A new CLI is added in the APN Profile mode to provide configurability at MME to accept or reject GBR and Non-GBR dedicated bearers. This control is applied on S11 as well as NAS. The relevant procedures are Create Bearer Request from S-GW and Bearer allocation request from UE. The MME differentiates GBR and Non-GBR dedicated bearers as follows: GBR Bearers - QCI value ranges from 1 to 4; Non-GBR bearers - QCI value ranges from 5-9. Note: Handling of multiple bearers in a Create Bearer request from S-GW for Partial accept/reject of GBR/Non-GBR dedicated bearers is a current limitation.
Command Changes

qos pgw-upgrade

This command includes the new `pgw-upgrade` keyword. This configures the action to be taken when the MME receives a QoS upgrade from P-GW for Non-GBR bearers.

```
configure
  apn-profile profile_name
    qos pgw-upgrade non-gbr { accept | reject | locally-cap }
    [ remove ] qos pgw-upgrade non-gbr
end
```

Notes:
- By default, the MME accepts the P-GW upgraded QoS values for Non-GBR bearers.
- `accept`: The MME will accept the P-GW upgraded QoS values.
- `reject`: The MME will reject the P-GW upgraded QoS values.
- `locally-cap`: The MME compares QCI, ARP and ARP-PVI provided by P-GW to the local values of those parameters. If the values match, then accepts towards the PGW and use local values towards the UE/RAN for APN-AMBR and ARP-PCI. If the values do not match, the MME rejects the P-GW upgraded QoS values.
- The MME will set the sum of the APN-AMBR of all active APNs up to the value of the subscribed UE-AMBR, subject to the UE-AMBR restriction.
- In the case of an Attach Reject or PDN Connectivity Reject, the ESM failure cause “Operator determined barring” is used and the corresponding MME statistic is incremented.
- In the case of Update Bearer Request Reject, the EGTP cause “Request rejected” is used and the corresponding EGTP statistic is incremented.
- A new session disconnect reason `mme-qos-pgw-upgrade-reject(589)` has been introduced to indicate when QoS upgrade by P-GW is rejected by the MME during initial attach. The corresponding session disconnect reason statistics are incremented.

`dedicated-bearers`

This new command configures the MME to either accept or reject GBR and Non-GBR `dedicated` bearers.

```
configure
  apn-profile profile_name
    dedicated-bearers { gbr { accept | reject } | non-gbr { accept | reject } }
    [ remove ] dedicated-bearers { gbr | non-gbr }
end
```

Notes:
By default, the MME accepts GBR and Non-GBR dedicated bearers.

**accept**: The MME will accept GBR/Non-GBR dedicated bearers.

**reject**: The MME will reject GBR/Non-GBR dedicated bearers.

The MME differentiates GBR and Non-GBR dedicated bearers as follows: GBR Bearers - QCI value ranges from 1 to 4; Non-GBR bearers - QCI value ranges from 5-9.

In the case of a UE-initiated Bearer Resource Allocation Reject, the ESM cause “EPS QOS not accepted” is used and the corresponding MME bulk statistic is incremented.

In the case of a Create Bearer Request Reject, the EGTP cause “Service denied” is used and the corresponding EGTP bulk statistic is incremented.

**Performance Indicator Changes**

**show apn-profile full name** `<profile_name>`

This command has been updated as highlighted below to display the configuration of the `qos pgw-upgrade` and `dedicated-bearers` commands.

**APN Type**: Unknown

**QOS upgrade from PGW for non-gbr**

**Action**: accept/reject/locally-cap/Not Configured

**Dedicated bearers**

**GBR**: accept/reject/Not Configured

**Non-GBR**: accept/reject/Not Configured

**show session disconnect-reasons verbose**

The following disconnect reason is included in the output of this command. It tracks disconnects when a QoS upgrade by P-GW is rejected by the MME during initial attach.

- mme-qos-pgw-upgrade-reject(589)

**CSCup23821** - NPUMGR Restart causing MME enB SCTP failures and impact to SGs/S1AP

**Feature Changes**

**Statistics and Counters Enhancements**

New counters have been added to the output of the `show session subsystem facility mmemgr` command to display specific packet drop reasons at the MME/Mgr.
Several `show` commands now display enhanced information for more clarity and better understanding of any problem in the flow-id creation/deletion process by MMEMgr. Refer to the Performance Indicator Changes section below for complete details.

These enhancements provide additional information to troubleshoot synchronization issues between the MMEMgr and NPUMgr.

**Performance Indicator Changes**

### `show session subsystem facility mmemgr all`

The output of this command has been enhanced to display counters for the following packet drop reasons:

- Incorrect Length - Received PDU length at MED layer is less than Length value found after decoding the IP Packet.
- Oversized PDU - Received PDU length at MED layer is more than DBUF size (10K bytes).
- No Flow exists - There is no SCTP flow existing for the flowId received from underlying layer.
- Flow Inactive Ver - Flow entry is not Active when the message is received.
- Invalid IP Ver - IP Version of the IP packet is not matching with the IP version for the SCTP flow.
- Port Mismatch - Destination SCTP Port of the IP packet is not matching with the SCTP port for the SCTP flow.
- Invalid Protocol - Protocol type is not found to be SCTP in the IP header.

### `show mme-service enodeb-association path-info`

The output of this command has been enhanced to display the Flow Id at the MMEMgr level.

- Flow Id

### `show mme-service enodeb-association full all`

The output of this command has been enhanced to display the Flow Id at the MMEMgr level.

- Flow Id

The output of this command has also been enhanced to display the individual path status along with flow information.

- Path Source IP Address
- Path Destination IP Address
- Path State
- Flow Id

### `show sgs-service vlr-status full`

The output of this command has been enhanced to display the SCTP flow id. For example:

```
Assoc Path State
192.80.80.41 192.80.80.33 UP 0x1b046db
```
CSCup29345 - Need MMEmgr CPU and Memory bulkstat counter for MME capacity monitoring

Feature Changes

Bulk Statistic Enhancements

**Previous Behavior:** CPU and memory related bulkstats were not available at the card-level for MMEMGR tasks for performance measurements.

**New Behavior:** The following information can now be collected:

- Total number of mmemgr tasks across all CPUs on this card.
- Average percentage of CPU utilization of all mmemgr tasks across all CPUs on this card.
- Average percentage of allocated memory utilization of all mmemgr tasks across all CPUs on this card.
- Maximum percentage of CPU utilization of the busiest mmemgr task across all the CPUs on this card.
- Maximum percentage of allocated memory utilization of the peak mmemgr task across all CPUs on this card.

Performance Indicator Changes

Card Schema

The following bulk statistics have been added to the Card schema to display card-level information for MME Manager tasks:

- task-mmemgr-num
- task-mmemgr-avgcpu
- task-mmemgr-avgmem
- task-mmemgr-maxcpu
- task-mmemgr-maxmem

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

Feature Changes

Delay in Processing Traffic After Restart

**Previous Behavior:** After an MME reboot or an SGs service configuration change, the S1 and SGs associations were not equally distributed across available MME Manager processes. On startup, the MME was starting to allocate traffic to individual MME Manager processes before all MME Manager processes were activated.

**New Behavior:** The MME now waits for all MME Manager processes to become available before processing traffic.
Performance Indicator Changes

**show session subsystem facility mmedemux verbose**

The following counter has been added to the output of the `show session subsystem facility mmedemux verbose` command.

This counter tracks the number of incoming packets dropped by the MME Demux subsystem (at S1 interface, coming from eNodeB) while waiting for all MME Managers to be activated (status = UP). The MME waits to start processing traffic only after the expected number of MME Managers are UP after an MME restart.

- Total number of packets dropped (Total MME Unavail)

**CSCup67478 - Reset-Req delete all sessions and send wrong feature-list to other HSSs**

Feature Changes

**HSS Reset Request Logic Enhancements**

**Previous Behavior:** When a Reset Request without a username (User-ID) was received from an HSS, the MME sent the Reset Request (including received Feature-List value) for all subscriber sessions irrespective of which HSS they were attached to earlier.

**New Behavior:** The MME now compares the received HSS's host name in the Reset-Request (RR) with all the local diameter-hss session's bound-host names and then sends the RR only for those sessions which are bound to that HSS host name.

This same change applies even if a RR is received with a User-ID, because the User-ID contains only the leading digits of IMSI and multiple IMSIs can match to the same User-ID. In this case some matched IMSI sessions may be bound to different HSS than the one which has sent the RR. So in this case also the RR is sent for those sessions which are bound to the HSS.

**CSCup71470 - Not interpreting RZC H6a AVP as a full hexadecimal value**

Feature Changes

**HSS Zone Code Format**

**Previous Behavior:** The MME always interpreted the received zone-code as an ASCII string (coded in hexadecimal representation) and converted it byte by byte to an integer value. For example, if the HSS sends the zone-code value as 3032, the MME converted this to 02 (ASCII value of 0 in Hex is 0x30, ASCII value of 2 in Hex is 0x32). As a result, the MME accepted zone-codes only within the range of 0 to 99.

**New Behavior:** By default, the MME now interprets the received zone-code value from HSS as a octet-string (2 bytes) which is coded in full hexadecimal representation. The MME now converts the entire 2 byte octet string coded in hexadecimal to integer value and it uses the same for validation for zone-code restriction feature. For example, if the HSS sends the zone-code value as 3032, MME converts this to 12338 (which is the equivalent of 0x3032).
A new command is provided in the HSS Peer Service Configuration Mode to specify the format of the zone-code value received from HSS to MME. This command allows the operator to maintain backward compatibility, where the MME interpreted the received zone-code value as an ASCII string.

**Customer Impact:** To maintain the previous behavior, where the MME interprets the zone-code value received from the HSS as ascii-string, the following command must be issued for each HSS Peer Service: `zone-code-format ascii-string`.

Refer to the following section for more information about this new command.

**Command Changes**

`zone-code-format`

This new command specifies the format of the zone-code value received from HSS to MME. The MME uses this configuration to interpret and convert the received zone-code value to an integer value and validate it against the list of allowed zone-code configured for the zone-code restriction feature.

This command is available within the HSS Peer Service Configuration Mode, and is configured per hss-peer-service.

```
configure
  context context_name
    hss-peer-service service_name
      zone-code-format { ascii-string }
      [ default ] zone-code-format
    end
```

**Notes:**

- **Important:** `service_name` must be unique across all contexts.
- By default, the MME interprets the zone-code from the HSS as an octet string.
- The `ascii-string` keyword option configures the MME to interpret the zone-code as an ascii string. This option is provided to maintain backward compatibility.

**Performance Indicator Changes**

`show hss-peer-service service all`

The following field has been added to the output of the `show hss-peer-service service all` command to display the configuration of the `zone-code-format` command.

The possible values are `octet-string` (default) and `ascii-string`.

- Zone Code format
CSCuq28652 - Low S1 signalling and low response for TAU requests

Feature Changes

Improved Handling During High Watermark in IMSIMGR

**Previous Behavior:** When a Session Manager facility reached the high watermark limit, the IMSI manager facility begins to drop MME calls.

**New Behavior:** Now when the high watermark limit is reached, subscribers will be moved to different Session Manager.

**Customer Impact:** Subscribers will no longer be dropped when the high watermark limit is reached on a given Session Manager.

CSCuq51479 - MME-CSFB: Handling of CSFB procedure for ongoing handover

Feature Changes

**Behavior Change for CSFB Procedure During Ongoing Handover**

**Previous Behavior:** If a Mobile Terminated (MT) Call received when an InterRAT, S1, or X2 Handover is in progress, the MME will process the SGS paging.

**New Behavior:** If a MT Call is received when an InterRAT Handover is in-progress, the MME will ignore the SGS paging.

If a MT call is received during ongoing S1/X2 handover, the MME will delay the procedure start until the handover completes.

In the case of a handover failure, the subsequent retransmission of SGS paging will trigger paging towards UE.

CSCuq74468 - MME TAU release cause with ESM failure when PGW is not responding

Feature Changes

**Separate Local Cause Mapping for Attach and TAU Procedures**

**Previous Behavior:** The default cause-code mapping whenever the error condition “GW not reachable” occurs is set to ESM-FAILURE for both Attach and TAU procedures. For a TAU procedure, the default cause to be sent should be NO-EPS-BEARER-CONTEXT-ACTIVATED in the reject message. There is no current capability to configure this cause code mapping on the MME. Also, there is no option to specify the cause-code mapping separately for Attach and TAU procedures, which results in assigning the same cause code for both.

**New Behavior:** The MME can now be configured to return separate cause codes for ATTACH and TAU procedures whenever the error condition “GW not reachable” occurs.
This can be configured within the Call Control Profile Configuration Mode as well as in the MME Service Configuration Mode. If a cause code mapping is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE.

The default cause-code mapping for “GW not reachable” for Attach procedures is still ESM-FAILURE, but for TAU procedures the default is now set to NO-EPS-BEARER-CONTEXT-ACTIVATED.

**Command Changes**

**local-cause-code-mapping gw-unreachable**

This command includes new optional keywords to configure the local cause code mapping separately for both Attach and TAU procedures. This enables an operator to configure the same cause-code for both Attach and TAU procedures, or separate cause-codes for Attach and TAU.

A new cause code keyword, no-bearers-active, is also now available for the GW unreachable error condition. This configures the MME to return the NO-EPS-BEARER-CONTEXT-ACTIVATED cause code in the reject message. This cause code can only be configured for TAU procedures, as it is not valid for Attach procedures.

**Call Control Profile Configuration Mode:**

configure
call-control-profile profile_name


    [ remove ] local-cause-code-mapping gw-unreachable [ attach | tau ]

end

**MME Service Configuration Mode:**

configure

    mme-service service_name


    [ default ] local-cause-code-mapping gw-unreachable [ attach | tau ]

end

Notes:
Important: service_name must be unique across all contexts.

- If a cause code mapping is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE.
- The default cause code mapping for Attach procedures is still ESM-FAILURE, but for TAU procedures the default is now set to NO-EPS-BEARER-CONTEXT-ACTIVATED.
- If the attach or tau optional keywords are not specified, the configured emm-cause-code will be sent for both Attach and TAU procedures.

Performance Indicator Changes

show call-control-profile full all

The output of this command now shows the local cause code mapping configuration for the gw-unreachable condition for both Attach and/or TAU procedures, as highlighted in the sample output below:

```
[local]hostname# show call-control-profile full all
...
Cause Code Mapping
GW unreachable Attach    : Network failure
GW unreachable TAU      : NO bearers active
STNSR NANPI IE during SRVCC Hand : Included
```

show mme-service all

The output of this command now shows the local cause code mapping configuration for the gw-unreachable condition for both Attach and/or TAU procedures, as highlighted in the sample output below:

```
[local]hostname# show mme-service all
...
PGW selection failure   : Network failure
GW unreachable Attach    : Network failure
GW unreachable TAU      : NO bearers active
NO active bearers       : NO bearers active
```
CSCuq86036 - Incorrect CLI text against Default bearer qos in "show apn-profile full"

Performance Indicator Changes

show apn-profile full all

The output for the `show apn-profile full all` command included a field labelled QoS Default BRR MBR. This caused ambiguity, as MBR is not associated with Default Bearer.

In this release, the field has now been changed to QoS Default BRR.
MME Enhancements for June 6, 2014

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
- ADC Enhancements
- CF Enhancements
- ECS Enhancements
- Firewall Enhancements
- GTPP Enhancements
- Lawful Intercept Enhancements
- InTracer Enhancements
- MVG Enhancements
- NAT Enhancements
- SNMP MIB Enhancements
- System & Platform Enhancements

**CSCts21153 - Change bulkstats variable for Retransmitted SCTP data chunks**

**Performance Indicator Changes**

**MME Schema**

The existing bulk statistic variable `sctp-retransdata-cookieack` has been renamed to `sctp-retransdata-data` to correctly reflect the information gathered.
CSCuh22222 - Allow the MME to construct the Destination Realm from the MNC/MCC

Feature Changes

Support for Constructing Dynamic Destination Realm for Foreign Subscribers

**Previous Behavior:** The MME could not construct a dynamic destination realm for foreign subscribers and instead always used the configured peer realm as the destination realm.

For a foreign subscriber, the MME does not know the HSS nodes in all the foreign PLMNs. In this case the MME routes S6a/S6d requests directed to foreign PLMNs via a Diameter Routing Agent (DRA) using only the destination realm. The DRA in turn routes the request to the correct HSS based on the destination realm. In order to accomplish this, the MME needs to dynamically construct requests to the DRA/HSS with a Destination Realm representing the foreign PLMN of the UE.

**New Behavior:** The MME now can derive the EPC Home Network Realm/Domain based on the user’s IMSI (MNC and MCC values) and use it as the Destination Realm.

A new HSS Peer Service Mode command has been introduced to enable this functionality. Refer to the following section “Command Changes” for more details.

Because MNCs can be 2 or 3 digits long, to provide the ability for an operator to configure the MCC and MNC of foreign PLMNs, the operator policy of the subscriber map is used to determine the MNC value and the length of the MNC.

Refer to *Configuring Dynamic Destination Realm Construction for Foreign Subscribers* in Chapter 2 of the MME Administration Guide for more information about configuring this feature.

Command Changes

dynamic-destination-realm

This new HSS Peer Service Mode command enables the MME to construct the destination realm using the MCC and MNC of foreign subscribers. By default, the MME uses the peer realm as destination realm.

configure

context ctxt_name

hss-peer-service service_name

[ default | no ] dynamic-destination-realm

end

**Important:** service_name must be unique across all contexts.

Note: For home subscribers, the MME will always use the configured peer realm as destination-realm, regardless if dynamic-destination-realm is enabled.
Performance Indicator Changes

show hss-peer-service service name

A new Destination Realm field has been added to the output of the show hss-peer-service service name command to display this configuration, either Configured Peer Realm (default), or Dynamic Realm.

Request Auth-vectors : l

Notify Request Message : Enable

Destination Realm : Dynamic Realm

CSCum83308 - MME Support for SGs Cause Code Mapping

Feature Changes

Suppress Call Reject for CS Call Paging Request to SMS-only Attached UE

This new configuration option enables the operator to configure whether to ignore the paging reject from the MME in case of sgs cs_call paging request for sms-only attached UE.

Previous Behavior: When the MME received a paging request for a CS call from MSC for an SMS-only attached device it would reject the paging request.

New Behavior: A new Call Control Profile command is provided to configure the MME to suppress the call reject in this scenario, instead of rejecting it. The default behavior is to reject the paging request.

Customer Impact: Allows the MME to process SGS CS call SMS-only paging requests for Ultra Card users where the same MSISDN is allocated to different IMSIs.

Command Changes

csfb

This command includes a new suppress-call-reject option to configure the Call Control Profile to suppress the call reject for SGs call paging for SMS-only attached devices.

configure

    call-control-profile profile_name

    csfb policy { not-allowed | not-preferred | sms-only | suppress-call-reject }

    remove csfb policy

    end

Performance Indicator Changes

show call-control-profile full name
This command now displays if the specified Call Control Profile is configured to suppress call rejects for SGs SMS-only attached devices.

CSFB Restrictions

SMS Only : FALSE
Not Allowed : FALSE
Not Preferred : FALSE
Suppress Call Reject : TRUE

CSCun94236 - MME uses wrong sec keys during 3g to 4g IRAT leading to SOS

Feature Changes

Behavior Change for 3G to 4G IRAT for Multiple Subscribers with Same GUTI

Previous Behavior: During a 3G to 4G IRAT where the device reports both a 3G identity (Mapped GUTI) and a 4G identity (Additional GUTI), and where the MME is able to retrieve profile information from both the 3G (SGSN Ctx Transfer) and 4G identity (mme db record), the MME uses the incorrect security keys in the Authentication Request message. As a result, the UE was sending auth-failure (mac-failure). This leads to TAU Reject with cause "Illegal UE", invaliding the SIM card and forcing the device into SOS until power cycled.

This issue is seen when multiple subscribers (a purged subscriber from MME and another detached subscriber) are having the same GUTI, and the purged subscriber comes back with the same addl-guti.

New Behavior: The MME now purges outdated data about subscriber and uses IMSI received from SGSN in above scenario. Correct authentication vectors are used, which avoids the auth-failure (mac-failure) from UE.

Additionally, the reject cause in case of auth-failure (mac) from MME is changed to "MS identity cannot be derived by the network".

Customer Impact: This updated cause code will prevent subscribers from being moved to SOS state.

CSCuo45960 - If both ipv4 & ipv6 GGSN addr available, MME to fwd ipv4 addr to SGSN

Feature Changes

Behavior Change When MME Receives Both IPv4 and IPv6 P-GW Addresses

Previous Behavior: The MME sent only one P-GW (IPv6) address in the Context Response and Forward Relocation Request when it had received both IPv4 and IPv6 addresses in the Create Session Response. This is applicable for Gn, S3 and S10 interfaces.

The MME displayed only one P-GW control and data address in the output of show mme-service session full.
New Behavior: The MME now sends both P-GW addresses in the Context Response and Forward Relocation Request when it has received both IPv4 and IPv6 addresses in the Create Session Response. This is applicable for the S3 and S10 interfaces.

For the Gn interface, if both addresses are received, the MME sends the P-GW address based on the peer-address type. Also, when the peer Gn-SGSN is resolved using DNS for Forward Relocation Request, the MME will send only the P-GW/GGSN IPv4 address even if it has knowledge of both.

The MME now also displays the IPv4 and IPv6 addresses for P-GW control and data teid in the output of `show mme-service session full`.

Customer Impact: Both addresses or address based on peer-address type would be sent.

Performance Indicator Changes

show mme-service session full

The MME now displays both the IPv4 and IPv6 addresses (if available) for P-GW control and data teid in the output of the `show mme-service session full` command, for example:

PDN Type: IPv4

PGW IPv4 Address: 11.7.1.1

PGW IPv6 Address: 2002::b07:101
MME Enhancements for March 31, 2014

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
- ADC Enhancements
- CF Enhancements
- ECS Enhancements
- Firewall Enhancements
- GTPP Enhancements
- Lawful Intercept Enhancements
- InTracer Enhancements
- MVG Enhancements
- NAT Enhancements
- SNMP MIB Enhancements
- System & Platform Enhancements

**CSCun23099 - STN-SR IE encoding is incorrect on Sv interface**

**Feature Changes**

**Inclusion of NANPI in STN-SR from HSS**

**Previous Behavior:** The MME did not include the Nature of Address and Numbering Plan Indicator (NANPI) in the Session Transfer Number for Single Radio Voice Call Continuity (STN-SR) IE on Sv interface in PS to CS request to MSC server and Forward Relocation request to peer-SGSN/peer-MME.

**New Behavior:** In support of TS 29.280 V10.1.0, the encoding of the STN-SR IE on Sv interface now includes the NANPI from the HSS. The value of NANPI sent by the MME is 0x11.
Command Changes

**srvcc exclude-stnsr-nanpi**

In this release, the MME now includes the NANPI in STN-SR in PS to CS request to MSC server and Forward Relocation request to peer-SGSN/peer-MME.

The following new command has been introduced to maintain backward compatibility. When this command is issued, the MME excludes the NANPI from these requests.

```
configure
  call-control-profile profile_name
    [ remove ] srvcc exclude-stnsr-nanpi
end
```

Performance Indicator Changes

**show call-control-profile full name**

The following field has been added to the output of the `show call-control-profile full name profile_name` command to show the configuration of the `srvcc exclude-stnsr-nanpi` command, either “Included” (default) or “Excluded”.

```
STNSR NANPI IE during SRVCC Handover : Excluded
```

CSCun28592 - S6a Feature List AVP is hardcoded in MME

Feature Changes

**Feature-List AVP Value in Messages Sent to HSS**

**Previous Behavior:** The MME always sent the Feature-List AVP value as 67110415 (0x400060F) as specified in TS 29.272 (prior to Version 10).

**New Behavior:** To comply with TS 29.272 Version 10 which changed the position of the T-ADS bit, the value sent in the Feature-List AVP is now configurable using the existing `diameter update-dictionary-avps` command in the HSS Peer Service Configuration Mode.

If this command is configured using the `3gpp-r9` keyword, 0x400060f is sent.

If this command is configured using the `3gpp-r10` keyword, 0x800060f is sent.
MME Enhancements for January 31, 2014

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**
- **ADC Enhancements**
- **CF Enhancements**
- **ECS Enhancements**
- **Firewall Enhancements**
- **GTPP Enhancements**
- **Lawful Intercept Enhancements**
- **InTracer Enhancements**
- **MVG Enhancements**
- **NAT Enhancements**
- **SNMP MIB Enhancements**
- **System & Platform Enhancements**

**CSCud33786 - GnGp: sgtpc: Incoming RIM messages are not sent to target eNodeB**

**Feature Changes**

**Support for RIM Routing Address Type eNodeB**

**Previous Behavior:** The MME supported only "RNC Identifier" (0x01 - RNC Identifier) RIM routing address discriminator. When the MME received RAN Information Relay (RIM) over the Gn interface with Discriminator as "RNC Identifier" and a RIM Routing address IE containing an RNC Id, the MME mapped the RNC Id to eNodeB Id.

**New Behavior:** The MME now supports the "eNodeB" (0x02 eNodeB Identifier) Discriminator, and can now find the eNodeB based on the RIM Routing address IE pointing to target eNodeB.
The MME still supports the use of an RNC Identifier for a RIM Routing Address, and will continue to map it to an eNodeB ID.

**CSCug78485, CSCuj28520, CSCuj28539 - EMM/ESM Cause Codes in bulkstats/counters**

**Performance Indicator Changes**

**MME Schema**

The following new bulk statistics have been added in this release. These include more detailed statistics for Tracking Area Updates (separate statistics for Inter-MME TAU and Intra-MME TAU), and more detailed statistics on reject cause values for EMM and ESM procedures:

- `emm-msgtx-tau-inter-accept`
- `emm-msgtx-tau-inter-accept-retx`
- `emm-msgtx-tau-inter-accept-imsi-unknown`
- `emm-msgtx-tau-inter-accept-no-msc`
- `emm-msgtx-tau-inter-accept-nw-fail`
- `emm-msgtx-tau-inter-accept-congestion`
- `emm-msgtx-tau-inter-accept-no-cs`
- `emm-msgtx-tau-intra-accept`
- `emm-msgtx-tau-intra-accept-retx`
- `emm-msgtx-tau-intra-accept-imsi-unknown`
- `emm-msgtx-tau-intra-accept-no-msc`
- `emm-msgtx-tau-intra-accept-nw-fail`
- `emm-msgtx-tau-intra-accept-congestion`
- `emm-msgtx-tau-intra-accept-no-cs`
- `emm-msgtx-tau-csg-not-subscribed`
- `emm-msgtx-tau-eps-non-eps-not-allowed`
- `emm-msgtx-tau-inter-reject`
- `emm-msgtx-tau-inter-imsi-unknown-hss`
- `emm-msgtx-tau-inter-illegal-ue`
- `emm-msgtx-tau-inter-illegal-me`
- `emm-msgtx-tau-inter-eps-not-allowed`
- `emm-msgtx-tau-inter-network-fail`
- `emm-msgtx-tau-inter-decode-failure`
- `emm-msgtx-tau-inter-no-bearer-active`
- emm-msgtx-tau-inter-ue-identity-unk
- emm-msgtx-tau-inter-implicit-detached
- emm-msgtx-tau-inter-imei-not-accept
- emm-msgtx-tau-inter-roaming-restrict-ta
- emm-msgtx-tau-inter-plmn-not-allow
- emm-msgtx-tau-inter-no-suitable-cell-ta
- emm-msgtx-tau-inter-ta-not-allow
- emm-msgtx-tau-inter-no-eps-svc-plmn
- emm-msgtx-tau-inter-csg-not-subscribed
- emm-msgtx-tau-inter-eps-non-eps-not-allowed
- emm-msgtx-tau-intra-reject
- emm-msgtx-tau-intra-imsi-unknown-hss
- emm-msgtx-tau-intra-illegal-ue
- emm-msgtx-tau-intra-illegal-me
- emm-msgtx-tau-intra-eps-not-allowed
- emm-msgtx-tau-intra-network-fail
- emm-msgtx-tau-intra-decode-failure
- emm-msgtx-tau-intra-no-bearer-active
- emm-msgtx-tau-intra-ue-identity-unk
- emm-msgtx-tau-intra-implicit-detached
- emm-msgtx-tau-intra-imei-not-accept
- emm-msgtx-tau-intra-roaming-restrict-ta
- emm-msgtx-tau-intra-plmn-not-allow
- emm-msgtx-tau-intra-no-suitable-cell-ta
- emm-msgtx-tau-intra-ta-not-allow
- emm-msgtx-tau-intra-no-eps-svc-plmn
- emm-msgtx-tau-intra-csg-not-subscribed
- emm-msgtx-tau-intra-eps-non-eps-not-allowed
- emm-msgrx-attach-retx
- emm-msgrx-tau-retx
- emm-msgrx-tau-inter-req
- emm-msgrx-tau-inter-retx
- emm-msgrx-tau-intra-req
- emm-msgrx-tau-intra-retx
- emm-msgtx-attach-rej-opr-determined-barring (Note: Not supported in this release.)
- emm-msgtx-attach-rej-insuff-resources
- emm-msgtx-attach-rej-activation-reject
- emm-msgtx-attach-rej-svc-not-subscribed
- emm-msgtx-attach-rej-svc-temp-out-of-order
- emm-msgtx-attach-rej-protocol-error
- emm-msgtx-attach-rej-apn-restrict-incompatible
- esm-msgtx-pdnc-on-rej-opr-determined-barring (Note: Not supported in this release.)
- esm-msgtx-pdnc-on-rej-insuff-resources
- esm-msgtx-pdnc-on-rej-activation-reject
- esm-msgtx-pdnc-on-rej-svc-not-subscribed
- esm-msgtx-pdnc-on-rej-svc-temp-out-of-order
- esm-msgtx-pdnc-on-rej-protocol-errors
- esm-msgtx-pdnc-on-rej-apn-restrict-incompatible

show mme-service statistics

The following new counters have been added in this release. These include more detailed counters for Tracking Area Updates (separate counters for Inter-MME TAU and Intra-MME TAU), and more detailed counters on reject cause values for EMM and ESM procedures:

Total EMM Control Messages

Sent

ESM Failure
- Opr Determined Barring (Note: Not supported in this release.)
- Insufficient Resource
- Activation Rejected
- Svc Opt Tmp OutOfOrder
- Protocol Errors
- APN Restrict Incomt

Total EMM Control Messages

Sent
- TAU Accept Intra MME
- Retransmissions
- IMSI Unknown in HSS
- MSC Unreachable
- Network Failure
- CS Domain Not Available
- Congestion
- TAU Accept Inter MME
- Retransmissions
- IMSI Unknown in HSS
- MSC Unreachable
- Network Failure
- CS Domain Not Available
- Congestion
- TAU Reject Total
- CSG Not Subscribed
- EPS non-EPS not Allwd
- TAU Reject Intra MME
- IMSI Unknown in HSS
- Illegal UE
- Illegal ME
- EPS Not Allowed
- Network Failure
- IMEI not accepted
- Decode Failure
- No Bearer Active
- UE Identity Unknown
- Implicitly Detached
- Roaming Restricted TA
- PLMN not allowed
- TA not allowed
- No suitable cells in TA
- No EPS Svc in PLMN
- CSG Not Subscribed
- EPS non-EPS not Allwd
- TAU Reject Inter MME
- IMSI Unknown in HSS
- Illegal UE
- Illegal ME
- EPS Not Allowed
- Network Failure
- IMEI not accepted
- Decode Failure
- No Bearer Active
- UE Identity Unknown
- Implicitly Detached
- Roaming Restricted TA
- PLMN not allowed
- TA not allowed
- No suitable cells in TA
- No EPS Svc in PLMN
- CSG Not Subscribed
- EPS non-EPS not Allwd

**Total EMM Control Messages**

**Received**
- Retransmissions (for Attach Request)
- Retransmissions (for TAU Request Total)
- TAU Request Intra-MME
- Retransmissions
- TAU Request Inter-MME
- Retransmissions

**Total ESM Control Messages**

**Sent**

**PDN Connectivity Reject**
- Opr Determined Barring (Note: Not supported in this release.)
- Insufficient Resource
- Activation Rejected
- Svc Opt Tmp OutOfOrder
- Protocol Errors
- APN Restrict Incomt
CSCuj49578 - sctp link not established with sctp-sack-period 0 in sctp-param-template

Feature Changes

Configuration of SCTP Parameter Template sctp-sack-period

**Previous Behavior:** If the SCTP Parameter Template associated to the MME and SGs services has a sctp-sack-period configured as 0, the SCTP stack would not get initialized for the MME and SGs services.

**New Behavior:** When the sack period is configured as 0 for the associated SCTP Parameter Template to MME and SGs services, the sack period is now automatically configured as 10ms in order for the SCTP stack to be initialized.

CSCuj77490 - MME Incomplete Suspend Response towards SGSN via Gn (gtp-c v1)

Feature Changes

MME Response to SGSN Context Request with Suspend Header

**Previous Behavior:** When the MME received a valid GTPv1 suspend request, the SGSN Context Response would be sent without a suspend header. As a result, the SGSN never sent the ACK to MME, and the MME would retry the context response.

**New Behavior:** On receiving a GTPv1 context request with a suspend header, the MME now sends the SGSN Context Response with the complete “SGSN Context Response” with cause “Requested Accepted” (OK) and “Next Extension Header” of type “Suspend Response” (NOT OK). The message is sent only once on the Gn interface (and not retried).

CSCul43064 - IE 95/94 should not be included in case X2HO w/out SGW change

Feature Changes

S1AP Protocol Change During X2 Handover with no S-GW Relocation

**Previous Behavior:** During an X2 handover, the MME would always include all successfully switched bearers in the E-RAB To Be Switched in Uplink List IE of a Path Switch Request Acknowledge message, regardless of whether the uplink tunnel endpoint changed or not. However, there is at least one eNodeB implementation that takes the presence of the IE to mean that S-GW relocation is taking place, regardless of the contents of the IE, and if the eNodeB is not licensed for S-GW relocation, it will drop the connection if the IE is present. This results in calls always going idle immediately following an X2 handover with no S-GW relocation.

**New Behavior:** The MME now includes the E-RAB To Be Switched in Uplink List IE of a Path Switch Request Ack message when X2 handover with S-GW relocation is taking place. During an X2 handover with no S-GW relocation, the IE will not be present.

**Customer Impact:** X2 handovers with no S-GW relocation would not work with certain eNodeB implementations not licensed for S-GW relocation, because they assume that presence of the IE implies S-GW relocation. Also note that, if
an eNodeB implementation were to insist on the presence of the IE in all Path Switch Request Ack messages, X2 handover with no S-GW relocation would no longer work with this change.

**CSCub06765 - Overcharging protection**

**Feature Changes**

**Overcharging Protection**

Overcharging Protection helps in avoiding charging subscribers for dropped downlink packets while the UE is in idle mode. This feature helps ensure subscribers are not overcharged.

![Important: A valid license key is required to enable Overcharging Protection on the MME. Contact your Cisco Account or Support representative for information on how to obtain a license.](image)

Refer to the *Overcharging Protection* chapter of the *MME Administration Guide* for more information about this feature.

**Command Changes**

`policy overcharge-protection`

Use this command to enable or disable overcharging protection for this MME service. When enabled, the MME can detect and signal a Loss of Signal Contact to the S-GW which in turn informs the P-GW to stop charging for the UE.

```plaintext
configure

context context_name

    mme-service svc_name

        policy overcharge-protection slap-cause-code-group group_name

        [ default | no ] policy overcharge-protection

end
```

Notes:

- `group_name`: Specify the name of a preconfigured S1-AP Cause Code Group.
- When the received cause code from the eNodeB matches any the cause codes defined in this Cause Code Group, the MME sets the ARRL (Abnormal Release of Radio Link) bit in the Indication IE of the Release Access Bearer Request to the S-GW.
- Refer to the `cause-code-group` command in the *LTE Policy Configuration Mode Commands* chapter, and the `class` command in the *SIAP Cause Code Configuration Mode Commands* chapter of the *ASR 5x00 Command Line Interface Reference* for more information.
Performance Indicator Changes

show mme-service

The Overcharge Protection field has been added to the output of `show mme-service all` and `show mme-service name service_name` to display the configuration of this feature, either “Not configured” or showing the configured S1-AP cause code group name:

Policy Inter-RAT Ignore SGSN ContextID : Disabled
Policy S1-Reset : Idle-Mode-Entry
Overcharge Protection : Cause Code Group grpl
MME Enhancements for November 30, 2013

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
- ADC Enhancements
- CF Enhancements
- ECS Enhancements
- Firewall Enhancements
- GTPP Enhancements
- Lawful Intercept Enhancements
- InTracer Enhancements
- MVG Enhancements
- NAT Enhancements
- SNMP MIB Enhancements
- System & Platform Enhancements

**CSCui50770 - NW Shared mme allocating wrong plmn in GUTI during TAU after 3g/4g srns**

**Feature Changes**

**GUTI Reallocation for PLMN Change**

**Previous Behavior:** UE initiated procedures with GUTI (like TAU or Service Request) fail if the UE does a 3G to 4G SRNS procedure earlier, in a network shared PLMN. This occurred only if the UE/eNobeB is from a PLMN that is network shared in MME. Any procedures involving GUTI were rejected with cause "CANNOT DERIVE MS IDENTITY".
New Behavior: The MME now triggers a GUTI relocation for this scenario and a new GUTI is allocated for the PLMN change.
MME Enhancements for September 30, 2013

MME Feature Changes as of September 30, 2013

This section provides information on MME feature changes in release 15.0.

**Important:** For more information regarding features in this section, refer to the *MME Administration Guide* for this release.

New MME Features

This section identifies new MME features available in release 15.0.

**Attach Rate Throttling**

This feature enables operators to limit the rate at which the MME processes new connections (attaches, TAU requests, and forward relocation requests) which in turn reduces the signaling on the external nodes.

See the `network-overload-protection mme-new-connections-per-second` command for more information.

**CSFB/SGS Bulk Statistics and Counters**

New Circuit-switched fallback statistics and counters have been introduced in this release. Refer to the *New MME Bulk Statistics* and *show mme-service statistics* sections for more information.

**Enhancements in Support of 3GPP 29.118 Release 10**

The following enhancements have been introduced to support Release 10.9.0 of 3GPP 29.188: Visitor Location Register (VLR) SGs interface specification:

- Support is added for a new SGs message SGsAP-SERVICE-ABORT-REQUEST as defined in the 3GPP specification. This SGs message is sent by MSC/VLR to MME to abort an ongoing CS service fallback for mobile terminating CS voice call. Upon receiving this message MME is required to abort the CS service fallback for the specified UE. No additional configuration is needed to support this functionality. Refer to the *Modified MME Bulk Statistics* and *Modified MME Output Fields* section of this document for more information.

- Support is added for configuration of the T13 Timer under the SGs service. Refer to the *Modified MME Commands* section of this document for more information.

**MME Support on ASR 5500 Platform**

The MME service can now be deployed on the ASR5000 and ASR5500 platforms. The same set of features are available across both platforms, giving operators flexibility in the choice of platform based on scale and not based on function.

**SRVCC Enhancements**

The following SRVCC-related enhancements are included in this release:
• The MME now supports MSC pools for load balancing and intelligent selection of MSC servers based on PLMN and/or IMSI hash values. Up to 24 MSC servers can now be defined per MME service.

• The MME now allows an administrator to place one or more MSC server in maintenance mode. This action removes the MSC server as a possible selection target.

• Support for IMS Centralized Service call handling as specified in 3GPP TS 29.280, enabling call flow handling for advanced scenarios.

• Support for GTP echo path management messages as defined in 3GPP TS 29.280.

• Support for Emergency call support.

Modified MME Features

This section identifies MME features modified in release 15.0.

Configurable Cause Code Mapping Enhancements

For the errors that are encountered during EMM procedures, the cause codes sent by the MME dictate actions on the UE. This feature provides improved flexibility and finer control of UE behavior during error conditions

**Previous Behavior:** The MME allowed configuration of EMM cause codes for the following conditions:

• APN mismatch
• Congestion
• New call policy restriction
• Restricted zone code.

**New Behavior:** The following additional conditions can now be mapped to specific cause codes at the Call Control Profile level and the MME Service level:

• Authentication failure
• Context transfer from MME failure
• Context transfer from SGSN failure
• HSS unavailable
• GW not reachable
• No active bearers
• Peer node resolution failure
• P-GW selection failure
• S-GW selection failure

VLR down and VLR unreachable condition cause codes are also now configurable in at the MME Service level in this release.

Deactivate Bearer Request During Additional PDN Disconnect

**Previous Behavior:** When a target eNodeB sends a path switch request, the MME did not send a deactivate bearer request to the new eNodeB even though the PDN disconnect request is sent to the MME.

**New Behavior:** In this scenario, the MME will not send a Deactivate Bearer Request.
The MME will keep track of the bearers listed in the Path Switch Request with a bitmask. When sending the Path Switch Ack, the MME will check the bitmask and place any bearers no longer present on the E-RAB To Be Released List.

In the Path switchreq-ack, the ErabtoBeReleased list IE will be populated with the particular RAB id.

**Enhanced Paging Initiation Event Statistics**

**Previous Behavior:** The MME reported Paging Initiation Event counters and statistics without regard to the paging trigger.

**New Behavior:** The ‘show mme-service statistics’ command now displays Paging Initiation Events per paging trigger: PS Events, CS Voice Events, CS SMS Events, and CS Other Events. Refer to the ‘show mme-service statistics’ command in the *New MME Output Fields and Counters* section for more information.

New statistics have been introduced in the MME schema to track Paging Initiation Event statistics based on different paging triggers: PS Events, CS Voice Events, CS SMS Events, and CS Other Events. Refer to the *New MME Bulk Statistics* section for more information.

**Enhancements in Support of 3GPP 29.272 Release 10**

The MME now provides the following support for Release 10 of 3GPP 29.272:

- The MME shall be able to receive new STN-SR (session transfer number for SR-VCC) info from the HSS as needed and to handle STN-SR.

**Enhancements in Support of 3GPP 29.274 Release 10**

The MME now provides support for Release 10 of 3GPP 29.274, including:

- Modifications in support of 29.274 CR-930 (C4-111596): Fix SRVCC related data transfer between MMEs/SGSNs.
- Modifications in support of 29.274 CR-1002 (C4-112195): Extended IE handling when received fields are less than expected fields.
- Modifications in support of 29.274 CR-844 (C4-110882): Serving Network IE.

**Enhancements in Support of 3GPP 29.280 Release 10**

The MME now provides the following support for Release 10.9.0 of 3GPP 29.280: Sv Interface (MME to MSC, and SGSN to MSC) for SRVCC:

- Support is added for IE Service Area Identifier as described in Section 6.12.

**Foreign GUTI DNS Control**

This feature allows customers to gain some savings on signaling by avoiding DNS request attempts to foreign PLMNs if a foreign-plmn-guti is not allowed.

**Previous Behavior:** Previously, all Attach and TAU Requests containing a foreign GUTI would result in a DNS lookup for the peer MME or SGSN, followed by an S10, S3 or Gn/Gp Identification or Context Request. This could result in significant delay when the GUTI is from a foreign PLMN, which the local MME cannot access.
New Behavior: This enhancement allows for a new configuration that can be used to apply restrictions on new foreign-plmn-guti. The behavior for Attach and TAU Requests with a foreign GUTI from a local PLMN (either the MME’s own PLMN or a network sharing PLMN) has not been changed.

See the **foreign-plmn-guti-mgmt-db** and **plmn** commands in this chapter for configuration information.

Inter-RAT GW Co-location Selection Improvements

In previous releases, node selection on the MME relied on DNS NAPTR procedures for node discovery as defined by 3GPP. Co-location of S-GW and P-GW was only possible when FQDNs are known for both S-GW and P-GW. During Gn/Gp handoffs, the P-GW is anchored and the S-GW alone needs to be selected. The MME does not learn the P-GW-FQDN from the old SGSN. As a result, selection of an S-GW co-located with the already anchored PGW is not viable.

This feature enhances the MME’s node-selection logic to ensure the selection of co-located S-GW with the anchored P-GW during Gn/Gp handoffs. The MME will construct the APN FQDN based on the APN name received from old SGSN. The MME performs DNS queries for both TAI-FQDN (for S-GW) and APN-FQDN (for P-GW) and constructs a list of node-pairs, sorted in the order of highest degree match, anchors the P-GW-node matching the IP address received from old-SGSN and then selects the S-GW following the same principles of node-selection. This results in the selection of a co-located S-GW (if present), or in the selection of a topologically closer S-GW.

This feature ensures that the load balancing and colocation benefits on the bearer plane are maintained across Inter-RAT HO scenarios.

Refer to the **policy inter-rat** command in the Modified MME Commands section of this document for more information.

Lawful Intercept Enhancements

When Camp-on is configured, the MME now sends an Session Event Active signal to the Lawful Intercept server when starting an interception for an active subscriber.

Location Services

The MME now supports additional Location Services (LCS) functionality:

- MT-LR procedures from the GMLC with client type of Lawful Intercept and Emergency services.
- Network Induced (NI-LR) procedures for Emergency PDN Connect and Emergency Attach, and Inbound relocation with emergency PDN (through TAU or SRNS).
- Circuit Switch Fallback (CSFB): When a UE is combined attached to the MME, and the CSFB registration is not for SMS-only services, the MME shall page UE on receipt of an SGs page with LCS Client identity.

Multiple Attach Request Handling

The MME now complies with 3GPP TS 24.301 for Attach Request collisions as follows:

- A second attach coming in an INITIAL UE message aborts the ongoing auth/pdn-connect procedures only when the Attach Request has IE changes.
- Mobile-ID is no longer considered in the Attach Req NAS message comparison.

Multiple MMEC Configuration in S1 Setup

Previous Behavior: Each MME in an MME pool is uniquely identified by one MME code (MMEC), which is used to build the GUTI assigned to the users attaching on that MME. In previous releases, only a single MMEC and MMEGI could be configured for a given MME service.
New Behavior: In this release, an additional configuration option allows the operator to indicate a list of served MMECs, in addition to the one assigned to the MME service. The complete list is notified to the eNodeB as Served MMECs in the S1 Setup Response. This aids the eNodeB in selecting a collocated MME during 3G to 4G handover events.

Refer to the `inter-rat-nnsf` command in the `Modified MME Commands` section for more information.

New SNMP Notifications

In Release 14.0, new SNMP traps were added to track the availability of VLR associations. (VLRAIAssocDown/VLRAIAssocDownClear and VLRAAsscUp/VLRAssocDown), where:

- VLRAssocDown - is sent when an association of a VLR is down.
- VlrAllAssocDown - is sent when all associations of all VLRs are down.

In this release, two new traps are added to indicate a condition where all SCTP associations to a specific VLR are down (VLRDwn) and when a down VLR comes back up (VLRUp).

- starVLRUp
- starVLRDwn

Two new SNMP traps have been introduced in this release to indicate a condition when new MME call are being rejected or dropped, and when this condition has been cleared and the MME is accepting new calls again.

- starMMENewConnectionsDisallowed
- starMMENewConnectionsAllowed

In the MME, new connections are setup for the following events

- UE initiated initial attach
- UE initiated inter-node TAU request requiring context transfer from old MME/SGSN
- Peer SGSN/MME initiated forward relocation request via Gn/S10/S3

Note that the congestion control feature generates its own set of traps to indicate/clear a congestion condition. However, if new connections are being disallowed due to congestion, both sets of traps may be generated.

S-GW Change Fallback Enhancements

Previous Behavior: In previous releases, the MME supported S-GW reselection and fallback if path-failure was detected while waiting for S11 create session response during initial attach procedure. S-GW fallback was not supported during any other procedures.

New Behavior: This feature has been enhanced to add detection of S-GW failure, and reselection and fallback for the S11 Create Session Response for S-GW relocation during X2 Handover, S1 Handover, and Idle mode Tracking Area Update procedures.

If DNS returns more than one S-GW candidate, and the MME sends Create Session Requests for all of the PDNs to the first S-GW and receives either no response or a failed response from the S-GW (meaning the CS bit in the Cause IE is set to 0) for all of the PDNs, the MME will then try sending Create Session Requests for all PDNs to the second S-GW. The MME will continue trying all candidate S-GWs until one of the following conditions are met:

1. A successful Create Session Response is received for at least one of the PDNs.
2. A failed Create Session Response is received from the P-GW (meaning the CS bit in the Cause IE is set to 1) for at least one of the PDNs.
3. The S-GW candidate list from DNS is exhausted
4. The procedure guard timer times out.

This functionality ensures that the calls are not disconnected due to S-GW failure or maintenance.

**S-GW Relocation Information Displayed in mme-service session Output**

**Previous Behavior:** Show commands did not show some information related to S-GW relocation procedures.

**New Behavior:** `show mme-service session full all` now shows S-GW control TEID, MSC_2, MSC_3, supported codecs and bearer deletion status.

**S1-AP Initial Context Setup Failure Handling Enhancements**

**Previous Behavior:** In previous releases, if the eNodeB returns an Initial Context Setup failure during service request procedure, the MME would detach the UE without signaling to the eNodeB and UE.

If the eNodeB returned an Initial Context Setup failure during a TAU procedure, the MME would move the UE to IDLE MODE without signaling to the eNodeB and UE.

**New Behavior:** The behavior of the MME for this scenario is now configurable.

For Initial Context Setup failure during a service request or extended service request, the MME can now move the UE to idle mode (instead of detaching the UE), as well as configure a list of cause codes that would move the UE to ECM_IDLE.

For Initial Context Setup failure during a TAU procedure, the MME can now detach the UE (instead moving the UE to idle mode), as well as configure a list of cause codes that would detach the UE.

**SCTP Template - SCTP Max In Streams and Max Out Streams**

**Previous Behavior:** Max in-streams and max out-streams in MME service can be configured 1-16 by associating an SCTP parameter template.

**New Behavior:** Max in-streams and max out-streams in MME service is restricted to 2-16. When the SCTP parameter template is associated to MME service with in-streams or out-streams configured as 1, value 2 will be applied.

**SGs Architecture Enhancements: Intelligent EMM Information Delivery**

**Previous Behavior:** Currently the MME provides the EMM Network Identity and Time Zone (NITZ) information twice in the case where SGs is present. This occurs because the MME delivers the EMM information (based on its own settings) early in the attach cycle, immediately following the security procedures and prior to initiation of LU towards the MSS over SGs. Since the MSS also delivers EMM information shortly (~200-300ms) following delivery of the attach accept, the MME subsequently passes the new EMM information to the UE.

**New Behavior:** In cases when the UE performs combined registration, the MME now can be configured to give a preference to the NITZ information as configured on the MME, or give preference to the information received from the MSC.

- If no preference is indicated, the MME performs as indicated in the Previous Behavior section.
- If MME information is given preference, the MME shall always send its information, and ignore any MM Information messages send by the MSC.
- If the MSC information is given preference, in cases where a successful Location Update is performed to a MSC, the MME shall NOT send MME configured information to the UE, and shall transmit only MSC send information. In cases where a Location Update procedure is not required (for example, for UE that are
performing EPS only ATTACH), or in cases where the Location Update Procedure is unsuccessful, the MME shall send the MME configured information.

See the `policy attach` and `policy tau` commands in the *Modified MME Commands* section of this document for information about this setting.

The net effect of the new algorithm will be a slight delay in the delivery of the EMM information to the UE. This delay will be almost imperceptible to the end user.

This feature eliminates three negative side effects: (1) Unnecessary OTA signaling on every attach. (2) In the case where the content of the EMM information is different (network names, timezone or Daylight Savings offset), the users could see the change occur on the UE’s display. (3) For UE’s that prompt the user whether to accept network time on their device, this will prevent multiple prompts and any undesirable side effects should a second EMM message be received before the user took action on the first EMM message prompt.

**SGs Architecture Enhancements: Load Balancing of Outbound Messages**

**Previous Behavior:** The SGs architecture allows multiple SCTP associations to be created from the MME toward the VLR. This allows the VLR to send and receive messages on any of the associations. In previous releases, the MME was able to perform load balancing at the application level across multiple SCTP associations for inbound messages. However, on the outbound side, the MME sent all update messages on a single link.

**New Behavior:** In this release, the MME has been enhanced to ensure outbound load balancing is achieved. No command line interface or configuration changes are required for this new functionality.

**UE-AMBR Displayed in show mme-service db record**

**Previous Behavior:** The APN-AMBR associated to each of the APN was available in the output of ‘show mme-service db record’, but not the subscription AMBR

**New Behavior:** Max Req Bandwidth UL and Max Req Bandwidth DL fields have been added to display the UE AMBR upload and download throughput. Refer to the *New MME Field Outputs and Counters* section for more information.

**MME Command Changes as of September 30, 2013**

This section provides information on MME command changes in release 15.0.

**Important:** For more information regarding commands in this section, refer to the *Command Line Interface Reference* for this release.

**New MME Commands**

This section identifies new MME commands available in release 15.0.

**associate**

This new command associates a pre-configured location service (LCS) with an LTE emergency profile. This enables the associated location service to provide location information of emergency calls to the GMLC.

**configure**

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

associate location-service <location_svc_name>
end

cause-code-group

This new command creates a new cause code group, or specifies an existing cause code group and enters the S1AP Cause Code Group Configuration Mode.

This command has been added to support the S1-AP Initial Context Setup Failure Handling Enhancements functionality, as described in the New MME Features section of this document.

configure
lte-policy

cause-code-group group_name protocol s1ap
end

class

This new command configures the specific cause codes within an S1AP Cause Code Group.

This command has been added to support the S1-AP Initial Context Setup Failure Handling Enhancements functionality, as described in the New MME Features section of this document.

configure
lte-policy

cause-code-group group_name protocol s1ap
class { miscellaneous | nas | protocol | radio | transport } cause cause_no
end

foreign-plmn-guti-mgmt-db

This new this command creates a new, or enters an existing Foreign PLMN GUTI management database. This management database is used to create restrictions on foreign PLMNs, thereby avoiding DNS request attempts to foreign PLMNs.

See the LTE Policy Configuration Mode Commands and LTE Foreign PLMN GUTI Management Database Configuration Mode Commands chapter of the Command Line Reference for more information.

configure
lte-policy

foreign-plmn-guti-mgmt-db <db_name>
end
**hash-value**

This new command configures the selection of a Mobile Switching Center (MSC) server in a MSC pool area based on the hash value derived from the IMSI. See the MME MSC Server Pool Area Configuration Mode chapter of the Command Line Reference for more information.

```plaintext
configure
  context <context_name>
    mme-service <service_name>
      pool-area <pool_area_name> type hash-value
        hash-value { hash_value | range start_value to end_value } use-msc msc_id
      end
```

**inter-rat-nnsf**

This new command configures an NNSF (NAS Node Selection Functionality) entry to define a list of Served MMECs (MME codes) that is indicated to the eNodeB in the S1 Setup Response. This optional configuration is used to aid the eNodeB when selecting the MME for inter-rat handovers when the MME is co-located with an SGSN. See the MME Service Configuration Commands chapter of the Command Line Reference for more information.

```plaintext
configure
  context <context_name>
    mme-service <service_name>
      inter-rat-nnsf collocated-mme plmn-id mcc mcc_value mnc mnc_value group-id mme_group_id mme-codes mmec
    end
```

**mme disconnect**

This new command disconnects the SCTP connection to the specified peer eNodeB. This command can be used to remove stale eNodeB connections from the MME, even when no active SCTP connection exists.

```plaintext
mme disconnect sl-peer peer_ID [ graceful ] [ -noconfirm ]
```

**network-overload-protection mme-new-connections-per-second**

This command configures an attach rate throttle mechanism to control the number of new connections allowed on a per second basis. See the Global Configuration Mode Commands chapter of the Command Line Reference for more information.

```plaintext
configure
  network-overload-protection mme-new-connections-per-second _new_connections action
    attach { drop | reject-with-emm-cause { congestion | network-failure | no-suitable-cell-in-tracking-area } } tau { drop | reject-with-emm-cause { congestion | network-failure | no-suitable-cell-in-tracking-area } }
```
This new command creates and configures a foreign Public Land Mobile Network (PLMN) entry in the Foreign PLMN GUTI management database. This optional configuration is used to control the acceptance or immediate reject of Attach Requests and TAU Requests containing a GUTI from the specified PLMN.

See the LTE Foreign PLMN GUTI Management Database Configuration Mode Commands chapter of the Command Line Reference for more information.

```
configure
  lte-policy <context_name>
    foreign-plmn-guti-mgmt-db <db_name>
      plmn mcc { mcc_value | any } mnc { mnc_value | any } [ allow | reject ]
    end

plmn-id

This new command associates a Public Land Mobile Network (PLMN) identifier with a Mobile Switching Center (MSC) pool area. This PLMN is used to select an MSC pool area based on the target PLMN as specified in the SRVCC handover request.

See the MME MSC Server Pool Area Configuration Mode chapter of the Command Line Reference for more information.

```
configure
  context <context_name>
    mme-service <service_name>
      pool-area <pool_area_name> type { hash-value | round-robin }
        plmn-id mcc code mnc code
      end
```

policy service-request

This new command configures the behavior of the MME when it receives a initial context setup failure during a service request or extended service request procedure.

```
configure
  context <context_name>
    mme-service <service_name>
```

```
policy service-request initial-context-setup-failure slap-cause-code-group
  group_name action idle-mode-entry
end

pool-area

This new command creates a Mobile Switching Center (MSC) server pool area and enters the MME MSC Server Pool Configuration mode. See the MME MSC Server Pool Area Configuration Mode chapter of the Command Line Reference for more information.

configure
  context <context_name>
  mme-service <service_name>
    pool-area pool_area_name type { hash-value | round-robin }
  end

use-msc

This command associates a Mobile Switching Center (MSC) with a round-robin MSC pool area. See also the pool-area command and the MME MSC Server Pool Area Configuration Mode chapter of the Command Line Reference for more information.

configure
  context <context_name>
  mme-service <service_name>
    pool-area <pool_area_name> type round-robin
    use-msc msc_name
  end

Modified MME Commands

This section identifies MME commands modified in release 15.0.

associate

The foreign-plmn-guti-mgmt-db keyword has been added to this command to associate a Foreign PLMN GUTI management database with an MME Service.

configure
  context <context_name>
  mme-service <service_name>
associate foreign-plmn-guti-mgmt-db <db_name>
end

diameter

The update-dictionary-avps keyword has been introduced to specify which release (r10 or r9) of 3GPP 29.272 is to be used for the HSS peer service.

configure

context <context_name>

hss-peer-service <service_name>

diameter update-dictionary-avps
end

local-cause-code-mapping

The following new keywords have been introduced to define EMM cause codes for errors encountered during EMM procedures.

These commands can be issued in the Call-Control-Profile Configuration mode as well as the MME Service Configuration mode.

configure

call-control-profile <profile_name>

local-cause-code-mapping auth-failure
local-cause-code-mapping ctxt-xfer-fail-mme
local-cause-code-mapping ctxt-xfer-fail-sgsn
local-cause-code-mapping gw-unreachable
local-cause-code-mapping hss-unavailable
local-cause-code-mapping no-active-bearers
local-cause-code-mapping peer-node-unknown
local-cause-code-mapping pgw-selection-failure
local-cause-code-mapping sgw-selection-failure
end

configure

context <context_name>
mme-service <service_name>

local-cause-code-mapping auth-failure
local-cause-code-mapping ctxt-xfer-fail-mme
local-cause-code-mapping ctxt-xfer-fail-sgsn
local-cause-code-mapping gw-unreachable
local-cause-code-mapping hss-unavailable
local-cause-code-mapping no-active-bearers
local-cause-code-mapping peer-node-unknown
local-cause-code-mapping pgw-selection-failure
local-cause-code-mapping sgw-selection-failure
local-cause-code-mapping vlr-down
local-cause-code-mapping vlr-unreachable

end

If a cause code mapping is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signaled to the UE. See the local-cause-code-mapping commands in the MME Service Configuration Mode Commands chapter or in the Call Control Profile Configuration Mode Commands chapter for more information.

**MSC**

This command has been enhanced to allow configuration of multiple Mobile Switching Center (MSC) servers enhanced with SRVCC, as well as the ability to mark an MSC server offline for maintenance mode. See also the pool-area command and the MME MSC Server Pool Area Configuration Mode chapter of the Command Line Reference for associating these MSC servers with an MSC pool.

configure

context <context_name>

mme-service <service_name>

  msc msc_name ip-address ip_address { offline | online }

end

**Policy attach / Policy tau**

The policy attach and policy tau commands have been enhanced with new keywords to add the ability to configure to the delivery of EMM Information message to the UE based on a preference for the MME’s information: (prefer-mme) or the information sent by the MSC: (prefer-msc).
These commands do not cause a restart of the MME service. For TAU and ATTACH, the policy will apply to the next request to be processed by the MME. A change in policy affects processing of TAU requests from UE already attached on the MME.

```
command
  context <context_name>
    mme-service <service_name>
      policy attach set-ue-time enable [ prefer-mme | prefer-msc ]
      policy tau set-ue-time enable [ prefer-mme | prefer-msc ]
    end

policy inter-rat

The select-topologic-sgw keyword has been introduced to configure the MME to determine and select the topologically-closest S-GW to the P-GW for Gn/Gp handoff scenarios.

```
command
  context <context_name>
    mme-service <service_name>
      policy inter-rat select-topologic-sgw interface gn
    end

policy tau

This command has been enhanced with a new initial-context-setup-failure keyword to configure the behavior of the MME when it receives a initial context setup failure during a TAU procedure.

```
command
  context <context_name>
    mme-service <service_name>
      policy tau initial-context-setup-failure slap-cause-code-group group_name action detach-ue
    end

report-overload

This command has been enhanced to support two new action codes as specified in Release 10 of the 3GPP S1-MME Interface Specification. The following keywords have been added: permit-high-priority-sessions-and-mobile-terminated-services and reject-delay-tolerant-access.

```
command
lte-policy

    congestion-action-profile <profile_name>
        report-overload { permit-high-priority-sessions-and-mobile-terminated-services | reject-delay-tolerant-access } enodeb-percentage percent
    end

show lte-policy

A new keyword, cause-code-group has been added to display information about the Cause Code Groups configured in the LTE Policy mode.

    show lte-policy cause-code-group { name group_name | summary }

A new keyword, foreign-plmn-guti-mgmt-db has been added to display information about the Foreign PLMN GUTI management databases configured in the LTE Policy mode.

    show lte-policy foreign-plmn-guti-mgmt-db { name db_name | summary }

snmp trap

The following command has been modified to enable or disable generation of two new SNMP traps to indicate when a VLR goes down and when a down VLR comes up again.

    configure
        snmp trap { enable | supress } { VLRdown | VLRup }
    end

The following command has been modified to enable or disable generation of two new SNMP traps to indicate a condition new MME call are being rejected or dropped, and when this condition has been cleared and the MME is accepting new calls again.

    configure
        snmp trap { enable | supress } { MMENewConnectionsAllowed | MMENewConnectionsDisallowed }
    end

timer

To support 3GPP 29.118 Release 10.9.0, a new ts13 keyword is added to the timer command under the SGS service to control the retransmission interval for sending SGS message SGsAP-EPS-DETACH-INDICATION to MSC/VLR.

    configure
        context <context_name>
            sgs-service <service_name>
                timer ts13 value
Deprecated MME Commands

This section identifies deprecated MME commands that are no longer supported in release 15.0.

None for this release

MME Performance Indicator Changes as of September 30, 2013

This section provides information on MME performance indicator changes in release 15.0.

Important: For more information regarding bulk statistics and output fields and counters in this section, refer to the Statistics and Counters Reference for this release.

New MME Bulk Statistics

This section identifies new MME bulk statistics available in release 15.0.

The following bulk statistics are new in this release:

MME Schema

The following new Service Reject statistics are added to display statistics for specific cause codes.

- emm-msgtx-service-reject-no-brrs
- emm-msgtx-service-reject-no-csg
- emm-msgtx-service-reject-ta-no-allwd
- emm-msgtx-service-reject-no-roam-in-ta
- emm-msgtx-service-reject-no-cells-in-ta

The following new statistics display the Attempted/Success/Failures statistics for circuit-switched fallback (CSFB) calls.

- csfb-ue-voice-total
- csfb-ue-voice-success
- csfb-ue-voice-failures
- csfb-ue-sms-total
- csfb-ue-sms-success
- csfb-ue-sms-failures
- csfb-ue-detach-total
- csfb-ue-detach-success
- csfb-ue-detach-failures
- csfb-nw-voice-total
- csfb-nw-voice-success
- csfb-nw-voice-failures
The following ECM Paging Initiation counters have been expanded to display individual counters based on different paging triggers: PS Events, CS Voice Events, CS SMS Events, and CS Other Events.

- cs-voice-paging-init-events-attempted
- cs-voice-paging-init-events-success
- cs-voice-paging-init-events-failures
- cs-voice-paging-last-enb-success
- cs-voice-paging-last-tai-success
- cs-voice-paging-tai-list-success
- cs-sms-paging-init-events-attempted
- cs-sms-paging-init-events-success
- cs-sms-paging-init-events-failures
- cs-sms-paging-last-enb-success
- cs-sms-paging-last-tai-success
- cs-sms-paging-tai-list-success
- cs-other-paging-init-events-attempted
- cs-other-paging-init-events-success
- cs-other-paging-init-events-failures
- cs-other-paging-last-enb-success
- cs-other-paging-last-tai-success
- cs-other-paging-tai-list-success
- ps-paging-init-events-attempted
- ps-paging-init-events-success
- ps-paging-init-events-failures
- ps-paging-last-enb-success
- ps-paging-last-tai-success
- ps-paging-tai-list-success

The following new statistics have been added to display TAU with TA/LA updating and TAU with IMSI attach.

- tau-ta-la-attempted
- tau-ta-la-success
• tau-ta-la-success-eps
• tau-ta-la-failures
• tau-ta-la-sgw-change-attempted
• tau-ta-la-sgw-change-success
• tau-ta-la-sgw-change-success-eps
• tau-ta-la-sgw-change-failures
• tau-imsi-attempted
• tau-imsi-success
• tau-imsi-success-eps
• tau-imsi-failures
• tau-imsi-sgw-change-attempted
• tau-imsi-sgw-change-success
• tau-imsi-sgw-change-success-eps
• tau-imsi-sgw-change-failures

The following new statistics have been added to display ESM failures during ATTACH at the cause code level.

• emm-msgtx-attach-rej-unknown-apn
• emm-msgtx-attach-rej-gw-reject
• emm-msgtx-attach-rej-gw-auth-failed
• emm-msgtx-attach-rej-svc-not-supported
• emm-msgtx-attach-rej-svc-not-subscribed

This new bulk statistic has been introduced to track EPS Mobility Management disconnects where a request contains a foreign GUTI and where the MME is configured to reject such foreign GUTIs as defined in the Foreign PLMN GUTI Management Database (foreign-plmn-guti-mgmt-db) configured in the lte-policy mode and which has been associated with the MME service.

• emmdisc-foreignplmnreject

SGS Schema

• service-abortreq-tx
• service-abortreq-retx
• service-abortreq-rx

The following new bulk statistic has been introduced to track the number of Location Update Request timeouts (due to expiration of ts6-1 timer) encountered on the SGs service.

• localupd-timeout-rx

SGS-VLR Schema

• service-abortreq-tx
• service-abortreq-retx
• service-abortreq-rx
The following new bulk statistic has been introduced to track the number of Location Update Request timeouts (due to expiration of ts6-1 timer) encountered on the SGs service on a per-VLR basis.

- localupd-timeout-rx

**LCS Schema**

The new Location Services (LCS) schema has been introduced to provide operational statistics used for monitoring and troubleshooting of the LCS service and SLg interface for communication with the Gateway Mobile Location Center (GMLC).

**System Schema**

The following disconnect reason has been introduced to the System Schema to track the total number of sessions disconnected resulting from restrictions set in the Foreign PLMN GUTI Management Database (foreign-plmn-guti-mgmt-db) configured in the lte-policy mode and which has been associated with the MME service.

- disc-reason-534: mme-foreign-plmn-guti-rejected(534)

**Modified MME Bulk Statistics**

This section identifies MME bulk statistics modified in release 15.0.

**MME Schema**

The following bulk statistic has been added to display the total number of EMM Detach Request messages sent, with the reason “IMSI Detach”:

- emm-msgrx-imsi-detach

The following statistics will show decreases due to the new TAU with TA/LA updating and TAU with IMSI attach counters introduced in this release. Those values are no longer included in the following counters:

- tau-normal-attempted
- tau-normal-success
- tau-normal-failures
- tau-sgw-change-attempted
- tau-sgw-change-success
- tau-sgw-change-failures

**Deprecated MME Bulk Statistics**

This section identifies deprecated MME bulk statistics that are no longer supported in release 15.0.

The following bulk statistics are deprecated for this release:

**MME Schema**

- paging-init-events-attempted
- paging-init-events-success
- paging-init-events-failures
- paging-last-enb-success
- paging-last-tai-success
• paging-tai-list-success

New MME Output Fields and Counters

This section identifies new MME show command output fields and counters available in release 15.0.

show call-control-profile full name

The following fields have been added to display the emm-cause-code to be returned to the UE when the respective condition is detected. These settings are configured using the local-cause-code-mapping command.

• APN mismatch
• Auth failure
• PEER NODE unknown
• CTXT transfer fail SGSN
• CTXT transfer fail MME
• HSS unavailable
• SGW selection failure
• PGW selection failure
• GW unreachable
• NO bearers active

show hss-peer-service service name

The following field has been added to display the configuration of the diameter update-dictionary-avps command:

• Update-Dictionary-AVPs

show location-service statistics all

The following fields have been added to display statistics for NI-LR location service (LCS) messages on the SLg interface:

• LR Request
• LR Request Dropped
• LR Answer
• LR Answer Dropped
• LR Answer Timeout

show lte-policy cause-code-group

This command displays summary information about all Cause Code Groups configured in the LTE Policy mode, or configuration information regarding a specific Cause Code Group.

• Cause Code Group <name>
• S1AP Protocol
• class

**show lte-policy foreign-plmn-guti-mgmt-db**

This command displays summary information about all Foreign PLMN GUTI management databases configured in the LTE Policy mode, or configuration information regarding a specific Foreign PLMN GUTI management database.

- Foreign PLMN GUTI Management DB <name>
- PLMN

**show mme-service all**

The following fields have been added to display the emm-cause-code to be returned to the UE when the respective condition is detected. These settings are configured using the `local-cause-code-mapping` command.

- APN mismatch
- VLR down
- VLR unreachable
- Auth failure
- PEER NODE unknown
- CTXT transfer fail SGSN
- CTXT transfer fail MME
- HSS unavailable
- SGW selection failure
- PGW selection failure
- GW unreachable
- NO bearers active

The following field has been added to display the LTE Foreign PLMN GUTI Management Database to which this MME Service is associated. This management database is used to control the acceptance or immediate reject of Attach Requests and TAU Requests containing a GUTI from a specific PLMN.

- Foreign-PLMN-GUTI-Mgmt-DB

The following field has been added to display whether the MME is configured to determine and select the topologically-closest S-GW to the P-GW for Gn/Gp handoff scenarios. This field shows the configuration of the `policy inter-rat select-topologic-sgw` command.

- Policy Inter-RAT Select Topologic SGW

The following fields have been added to display the configured MME behavior when it receives an initial context setup failure during TAU procedures or during service request procedures. These fields show the configuration of the `policy tau initial-context-setup-failure` and `policy service-request initial-context-setup-failure` commands.

- Initial Context Setup Failure- TAU
- Initial Context Setup Failure-Svc Req
show mme-service db record

The following fields have been added to display the UE AMBR upload and download throughput.

- Max Req Bandwidth UL
- Max Req Bandwidth DL

This information is now available in the following commands:

```bash
show mme-service db record imsi <imsi>
show mme-service db record call-id <call-id>
show mme-service db record guti <guti>
```

show mme-service session full all

The following fields have been added to display information for S-GW relocation procedures.

- SGW Control TEID
- Supported Codec List
- Mobile Station Classmark 2
- Mobile Station Classmark 3
- Marked for Deletion

show mme-service statistics

The following fields have been added to display the Network Induced Location Request (MT-LR) Location Services (LCS) attempts/successes/failures associated with all MME services on the system.

- Network Induced Location Request:
  - Attempted
  - Success
  - Failures

The following fields have been added to display Attach reject with cause code ESM failure.

- ESM Failure:
  - Unknown or Missing APN
  - Rejected By PGW/SGW
  - Authentication Failed
  - Svc Opt Not Supported
  - Svc Opt No Subscribed

The following new counters are available to display the Attempted, Success, Success EPS Only, and Failure statistics for TAU with TA/LA updating and TAU with IMSI attach:

- Combined TA/LA Updating without SGW Relocation
- Combined TA/LA Updating with SGW Relocation
- TAU with IMSI attach without SGW Relocation
• TAU with IMSI attach and SGW Relocation

The following field has been added to display the total number of EMM Detach Request messages sent, with the reason “IMSI Detach”:

• IMSI Detach

The following ECM Paging Initiation counters have been expanded to display individual counters based on different paging triggers: PS Events, CS Voice Events, CS SMS Events, and CS Other Events.

• Paging Initiation Events for PS Events:
  • Attempted
  • Success
  • Failures
  • Success at Last n eNB
  • Success at Last TAI
  • Success at TAI List

• Paging Initiation Events for CS Voice Events
  • Attempted
  • Success
  • Failures
  • Success at Last n eNB
  • Success at Last TAI
  • Success at TAI List

• Paging Initiation Events for CS SMS Events
  • Attempted
  • Success
  • Failures
  • Success at Last n eNB
  • Success at Last TAI
  • Success at TAI List

• Paging Initiation Events for CS Other Events
  • Attempted
  • Success
  • Failures
  • Success at Last n eNB
  • Success at Last TAI
  • Success at TAI List

The following new fields are added to Service Reject to display statistics for specific cause codes.
- Roaming Restricted TA:
- No suitable cells in TA
- TA Not Allowed

The following new counters are added to display the Attempted/Success/Failures statistics for circuit-switched fallback (CSFB) calls.

- CSFB Statistics:
  - UE Initiated Voice Procedures
  - NW Initiated Voice Procedures
  - UE Initiated SMS Procedures
  - NW Initiated SMS Procedures
  - UE Initiated IMSI Detaches
  - NW Initiated IMSI Detaches

**show session disconnect-reasons**

If a session containing a foreign GUTI is rejected due to its PLMN being present in the Foreign PLMN GUTI Management Database, the following session disconnect reason is incremented.

- mme-foreign-plmn-guti-rejected(534)

**show sgs-service all**

The following field has been added to show the configuration of the new SGs service ts13 timer value:

- Timer Ts13

**show sgs-service statistics all**

The following counter has been added to show the number of SGsAP-SERVICE-ABORT-REQUEST messages transmitted, retransmitted and received:

- Service Abort Request

The following counter has been introduced to track the number of Location Update Request timeouts (due to expiration of ts6-1 timer) encountered on the SGs service.

- Location Update Timeout Rx

**show sgs-service vlr-status full**

The following counter has been introduced to track the number of Location Update Request timeouts (due to expiration of ts6-1 timer) encountered on the SGs service on a per-VLR basis.

- Location Update Timeout Rx

**Modified MME Output Fields and Counters**

This section identifies modified MME show command output fields and counters available in release 15.0.
show mme-service all

The following fields have been changed to show the configured preference for delivery of the EMM information message (prefer-mme or prefer-msc) for the set-ue-time keyword in the policy attach and policy tau commands:

- Set UE Time (attach processing)
- Set UE Time (TAU processing)

Deprecated MME Output Fields and Counters

This section identifies deprecated MME output fields and counters that are no longer supported in release 15.0.

show mme-service statistics

The existing “Paging Initiation Events” group of counters have been deprecated and replaced by the new fields in this release.

- Paging Initiation Events
- Attempted
- Success
- Failures
- Success at Last n eNB
- Success at Last TAI
- Success at TAI List
Chapter 15
MVG Changes in Release 15.0

This chapter identifies features and functionality added to, modified for, or deprecated from 15.0 MVG software releases.
MVG Enhancements for September 30, 2013

MVG Feature Changes as of September 30, 2013

This section provides information on MVG feature changes in release 15.0.

**Important:** For more information regarding features in this section, refer to the *MVG Administration Guide* for this release.

New MVG Features

This section identifies new MVG features available in release 15.0.

**MVG CAE Video Re-addressing Without Full TCP Proxy**

With this release, the MVG video re-addressing feature does not require a TCP proxy connection for the entire duration of the flow. The video re-addressing functionality towards CAE is invoked only on the first HTTP video request, and response. Thereafter, the rest of the packets do not need the proxy functionality, and TCP proxy is dynamically disabled as soon as a response packet is received from the CAE.

Once connection is setup with CAE and proxy is disabled, MVG still keeps monitoring all requests and inserts MVG x-headers to all requests (both video and non-video) being forwarded to CAE. X-headers are required for CAE to access the requested content from the Origin server (OS) if needed. MVG x-headers will be added to both pipelined and non-pipelined (both video and non-video) requests once connection is setup with CAE and proxy is disabled.

**MVG Platform Support**

The following are the platform support for the MVG CAE video re-addressing, and the MVG video pacing features:

- **CAE Video Re-addressing:** This feature is now qualified to run on the Cisco ASR 5000 chassis for PSC2 and PSC3 integrated with GGSN, P-GW, and SAE-GW (if MVG is running on P-GW) products. To use this feature in a combination of GGSN, P-GW, and HA products, MVG should run on GGSN or P-GW.

- **Video Pacing:** This feature is now qualified to run on ASR 5000 and ASR 5500 chassis integrated with GGSN, P-GW, SAE-GW (if MVG is running on P-GW), HA, and IPSG (ASR 5000 only) products. To use this feature in a combination of GGSN, P-GW, and HA products, MVG should run on GGSN or P-GW.

**MVG Interworking With Cisco Inlet CAE**

With this release, the Mobile Video Gateway Inline service is fully qualified to interwork with the Cisco Inlet Content Adaptation Engine (CAE) for video optimization and re-addressing.

**Dynamic Disabling of TCP Proxy**

With this release, TCP proxy can be disabled during the middle of the HTTP flow for the MVG CAE video re-addressing feature. The video re-addressing functionality towards CAE is invoked only on the first HTTP video request (connection establishment and x-header insertion), and response. As the rest of the flow to the CAE does not require a TCP proxy, it is disabled. This leads to the overall improvement of the system performance.
Video Pacing Qualification for Release 15.0

The video pacing feature enables mobile operators to limit the download speed of over-the-top, progressive download video (video clips provided to subscribers via HTTP downloads over TCP flows) so that their subscribers download just enough video content in time for smooth playback. By limiting the bit rate of progressive downloads to the actual encoded bit rate of each video clip, mobile operators can significantly reduce their air interface bandwidth usage. This feature is now qualified for the 15.0 Release.

CAE Video Re-addressing Qualification for Release 15.0

The Mobile Video Gateway can re-address HTTP video requests intended for video content Origin Servers (OS) toward the Cisco CAE for retrieval of optimized video content. The Cisco CAE is an optional component of the Cisco Mobile Videoscape. It functions in a video server cluster to bring additional optimization capabilities to the Mobile Videoscape. This feature is now qualified for the 15.0 Release.

New MVG x-headers for CAE Readdressing

Additional MVG x-headers are introduced with this release to insert into the HTTP header that is sent to the CAE. The following MVG x-headers are now introduced in 15.0 for MVG x-header insertion:

- x-congestion
- x-ToD
- x-forwarded-dest-addr-port

For a complete list of supported MVG x-headers, refer to the Mobile Video Gateway Administration Guide.

MVG X-Header Insertion After TCP Proxy Disabled

TCP proxy is disabled as soon as a response packet is received by MVG from CAE. For persistent connections with continuous requests from the UE, once a connection is established with the CAE for processing the first video request, TCP proxy is disabled and the connection with the CAE is kept active until the end of the flow. Both video and non-video requests are processed by a CAE that is capable of processing both types of requests. The MVG x-headers which are critical for the functionality of the MVG CAE re-addressing feature will be inserted to the packets even after TCP is disabled.

Modified MVG Features

This section identifies MVG features modified in release 15.0.

Video Optimization License Changes

The MVG CAE re-addressing feature requires MVG to insert extra x-headers like RAT, device type, user profile, time of day, and congestion level in the HTTP message before forwarding the request to the CAE.

**Previous Behavior:** In earlier releases, in addition to the ECS, and MVG (video optimization) licenses, a separate HTTP Header Enrichment license was required to use the ECS x-header insertion feature.

**New Behavior:** With this release, the MVG (video optimization) license includes limited support to x-header insertion. The MVG license now includes support for x-headers that are required by the MVG CAE re-addressing feature. For a complete list of supported x-headers, see the CAE Video Re-addressing section in the Mobile Video Gateway Administration Guide.
Important: For more information on the video optimization license, please contact your Cisco account representative.

MVG Command Changes as of September 30, 2013

This section provides information on MVG command changes in release 15.0.

Important: For more information regarding commands in this section, refer to the Command Line Interface Reference for this release.

New MVG Commands

This section identifies new MVG commands available in release 15.0.

None for this release.

Modified MVG Commands

This section identifies MVG commands modified in release 15.0.

insert

This command allows you to configure the x-header fields to be inserted in HTTP/WSP GET and POST request packets.

With this release the keywords `congestion-level`, `dest-server-ip-address-port`, and `time-of-day` have been added to the command in support of the CAE re-addressing feature.

```
configure

    active-charging service <service_name>

    xheader-format format_name

        insert xheader_field_name variable bearer { congestion-level | dest-server-ip-address-port | time-of-day }

    end
```

Deprecated MVG Commands

This section identifies deprecated MVG commands that are no longer supported in release 15.0.

None for this release.

MVG Performance Indicator Changes as of September 30, 2013

This section provides information on MVG performance indicator changes in release 15.0.
Important: For more information regarding bulk statistics and output fields and counters in this section, refer to the Statistics and Counters Reference for this release.

New MVG Bulk Statistics
This section identifies new MVG bulk statistics available in release 15.0.

New in the ECS Schema
The following bulkstats are added to the ECS shema towards the MVG CAE re-addressing feature:

- video-readdress-req-redirected
- video-readdress-res-redirected
- video-readdress-req-with-xheader-inserted
- video-readdress-upl-bytes-redirected
- video-readdress-upl-pkts-redirected
- video-readdress-dnl-bytes-redirected
- video-readdress-dnl-pkts-redirected
- video-readdress-req-charging-action-hit
- video-readdress-resp-charging-action-hit
- video-readdress-skipped-pipelined-reqs
- video-readdress-connect-failed-to-video-server
- video-readdress-load-balancer-failures
- video-readdress-flows-connected-to-video-server
- video-readdress-xhdr-insert-failed

Modified MVG Bulk Statistics
This section identifies MVG bulk statistics modified in release 15.0.
None for this release.

Deprecated MVG Bulk Statistics
This section identifies deprecated MVG bulk statistics that are no longer supported in release 15.0.

Deprecated in the ECS Schema
The following video optimization-related bulk statistics are deprecated for this release:

- video-opt-total-transrated
- video-opt-total-gzipped
- video-opt-total-mp4
New MVG Output Fields and Counters

This section identifies new MVG show command output fields and counters available in release 15.0.

**show active-charging**

The following counters have been added to the output of the `show active-charging charging-action statistics name charging_action_name` and the `show active-charging rulebase statistics name rulebase_name` commands for the CAE video re-addressing and dynamic TCP proxy disable features:

- CAE-Readdressing
  - Requests CAE-Readdressed
  - Responses CAE-Readdressed
  - Requests having xheader inserted

- video-opt-total-flv
- video-opt-transrated-sh263
- video-opt-transrated-h264
- video-opt-failed-sh263
- video-opt-failed-h264
- video-opt-failed-vcodec
- video-opt-total-input-bytes
- video-opt-total-input-bytes-sh263
- video-opt-total-input-bytes-h264
- video-opt-total-input-bytes-gzip
- video-opt-total-output-bytes
- video-opt-total-output-bytes-sh263
- video-opt-total-output-bytes-h264
- video-opt-total-output-bytes-gzip
- video-opt-avg-input-bitrate
- video-opt-avg-input-bitrate-sh263
- video-opt-avg-input-bitrate-h264
- video-opt-avg-output-bitrate
- video-opt-avg-output-bitrate-sh263
- video-opt-avg-output-bitrate-h264
- video-opt-avg-rate-reduction
- video-opt-avg-rate-reduction-sh263
- video-opt-avg-rate-reduction-h264
The following counters have been added to the output of the `show active-charging flows full` command for the CAE video re-addressing and dynamic TCP proxy disable features:

- **CAE Readdressing**
  - Requests CAE-Readdressed
  - Responses CAE-Readdressed
  - Requests having xheader inserted
  - Total connect failed to CAE
  - Total CAE-Readdressed Uplink Bytes
  - Total CAE-Readdressed Uplink Packets
  - Total CAE-Readdressed Downlink Bytes
  - Total CAE-Readdressed Downlink Packets
  - Flows connected to CAE
  - Proxy Disable Success
  - Proxy Disable Failed
  - Readdressed to
Modified MVG Output Fields and Counters

This section identifies modified MVG show command output fields and counters available in release 15.0.

None for this release.

Deprecated MVG Output Fields and Counters

This section identifies deprecated MVG output fields and counters that are no longer supported in release 15.0.

None for this release.
Chapter 16
NAT Changes in Release 15.0

This chapter identifies features and functionality added to, modified for, or deprecated from 15.0 NAT software releases.

**Important:** All functionality from Limited Availability Release StarOS Version 14.1 has been included in General Availability Release StarOS Version 15.0. The *Cisco ASR 5x00 Release Change Reference, Version 14.1*, details new feature descriptions and configuration, performance, and security changes for the 14.1 release.
NAT Enhancements for September 30, 2013

NAT Feature Changes as of September 30, 2013

This section provides information on NAT feature changes in release 15.0.

**Important:** For more information regarding features in this section, refer to the *Network Address Translation Administration Guide* for this release.

### New NAT Features

This section identifies new NAT features available in release 15.0.

**SIP ALG Support for NAT64**

SIP ALG is supported for NAT64 in this release. SIP packets can now undergo NAT64 translation.

SIP request and response packets contain IP addresses embedded in their headers. For SIP packets originating from an IPv6 network, the IP addresses will be in IPv6 format. The destination IPv4 network will not be able to process the SIP packets if these IPv6 addresses are not translated to their corresponding IPv4 addresses. Similarly, the IPv4 addresses coming from IPv4 network need to be converted to their corresponding IPv6 addresses. With this release, SIP ALG interworks with NAT to perform these translations so that SIP packet processing is unaffected at both IPv6 and IPv4.

**Server IP Address in Access Rule Definitions**

Access Rule Definitions now support Server IP address to avoid configuring multiple rule options as part of Firewall rules. With this release, the `ip server-ip-address` command is added in access ruledefs. If any address or host-pool range is specified as the server IP address, this address in the uplink direction will be treated as the destination address, and in downlink direction will be treated as the source address.

### Modified NAT Features

This section identifies NAT features modified in release 15.0.

**Enabling NAT**

**Previous Behavior:** NAT will be disabled by default if the assigned IP is already a public IP.

**New Behavior:** A new keyword `skip-nat-subscriber-ip-check` is added in this release. On enabling this option, the private IP check for the corresponding non-NAT pool will be skipped, while NAT will be enabled (if configured) for this pool although it is a public pool. The user can control enabling of NAT irrespective of whether the assigned IP is a private or public IP address. Refer to the `ip pool` command for more information.

**NAT Busyout**

When a NAT pool is busied out, no new calls will receive IP from the busied out pool. Only calls which have received IP from the pool prior to busy out will be using the IP. Busyout feature is now supported for both NAT and ordinary pools.
Previous Behavior: The Busyout feature was supported only for ordinary pools.
New Behavior: In this release, the Busyout feature is supported for NAT pools.

NAT Realm during IP allocation

Previous Behavior: NAT realm was displayed as part of the show subscriber full CLI command irrespective of whether IP is assigned from that NAT realm or not.
New Behavior: NAT realm will be now displayed only when IP is assigned and removed again when IP is released.

Network Broadcast for NAT Realms

Network broadcast support has now been extended for NAT pools using the include-nw-bcast option of the ip pool command in the Context Configuration mode. In earlier releases, only ordinary pools included network broadcast using the same include-nw-bcast option.

SIP ALG Behavior

As part of this feature, SIP ALG is made compatible with user-to-user authentication and processing 4xx responses as described in RFC 3261. A new command, sip advanced is added in the Active Charging Service Configuration mode to enable SIP ALG to maintain the same tag parameters (from and to tag) for Authorization or Proxy Authentication requests.

Previous Behavior: SIP ALG forwarded a re-invite request with credentials (sent by the client after the server responded with a 401 to the initial Invite request) with a new “From Tag” which is different from the “From Tag” added by SIP ALG for the initial Invite request. This was implemented as per section 19.3 of RFC 3261. As some SIP servers have strict policy implementations, calls are terminated due to this default behavior of SIP ALG.
New Behavior: In this release, the re-invite to 401 is sent with the same “From Tag” as the initial Invite request as defined in sections 8.1.3.5 and 22.2 of RFC 3261.

NAT Command Changes as of September 30, 2013

This section provides information on NAT command changes in release 15.0.

**Important:** For more information regarding commands in this section, refer to the Command Line Interface Reference for this release.

New NAT Commands

This section identifies new NAT commands available in release 15.0.

**ip server-ip-address**

This command configures an access ruledef to analyze user traffic based on server IP address.

```
configure
  active-charging service acs_service_name
  access-ruledef access_ruledef_name
```
[ no ] ip server-ip-address { operator { ipv4/ipv6_address | ipv4/ipv6_address/mask } | { !range | range } host-pool host_pool_name }

end

sip advanced

This command enables SIP ALG to maintain the same tag parameters (from and to tag) for Authorization or Proxy Authentication requests.

configure

active-charging service acs_service_name

sip advanced out-of-dialog-request retain-tag

end

Modified NAT Commands

This section identifies NAT commands modified in release 15.0.

ip pool

This command enables creation, configuration or deletion of IP address pools in the current context. A new keyword skip-nat-subscriber-ip-check is added to skip private IP address check for non-NAT pools. This can be configured only for non-NAT pools during call-setup if NAT is enabled for the subscriber. If NAT is disabled, this value is not considered.

configure

context context_name

ip pool pool_name { ip_address/subnet_mask | ip_address_mask_combo | range start_ip_address end_ip_address } [ skip-nat-subscriber-ip-check ]

end

show active-charging analyzer statistics

This command displays statistical information for protocol analyzers. A filter based on instance is added to show the statistics of the number of SIP-TCP or SIP-UDP calls.

show active-charging analyzer statistics [ name protocol_name [ instance instance_number ] [ verbose ] ] [ | { grep grep_options | more } ]

show active-charging firewall statistics

This command displays Active Charging Stateful Firewall statistics. The wide keyword is added to display all available information in a single wide line.

show active-charging firewall statistics [ wide ]
show active-charging flows

This command displays information for active charging flows. New optional keywords `call-id`, `control-connection`, and `firewall` are added to this command as filters to debug Firewall enabled flows.

```
show active-charging flows { all | [ call-id call_id ] [ control-connection { ftp | pptp | rtsp | sip | tftp } ] [ firewall { not-required | required } ] }
```

**show active-charging flows**

This command displays information for active charging flows. New optional keywords `imsi`, `msisdn`, `binding-info`, and `username` are added to this command as filters to debug Firewall/NAT enabled flows.

```
show active-charging flows { all | [ imsi imsi_value ] [ msisdn msisdn_num ] [ nat { not-required | required [ binding-info ] } ] [ username user_name ] }
```

**Deprecated NAT Commands**

This section identifies deprecated NAT commands that are no longer supported in release 15.0.

None for this release.

**NAT Performance Indicator Changes as of September 30, 2013**

This section provides information on NAT performance indicator changes in release 15.0.

**Important:** For more information regarding bulk statistics and output fields and counters in this section, refer to the *Statistics and Counters Reference* for this release.

**New NAT Bulk Statistics**

This section identifies new NAT bulk statistics available in release 15.0.

**New in the Context Schema**

The following bulk statistic is added in this release to display statistics for NAT and Bypass-NAT flows:

- nat-current-flows
- nat44-current-flows
- nat64-current-flows
- bypass-nat-current-flows
- bypass-nat-ipv4-current-flows
- bypass-nat-ipv6-current-flows

**New in the ECS Schema**

The following bulk statistics are added in this release to display statistics for SIP-TCP and SIP-UDP calls:
• sip-advanced-total-calls
• sip-advanced-udp-calls
• sip-advanced-total-udp-calls
• sip-advanced-tcp-calls
• sip-advanced-total-tcp-calls

Modified NAT Bulk Statistics
This section identifies NAT bulk statistics modified in release 15.0.
None for this release.

Deprecated NAT Bulk Statistics
This section identifies deprecated NAT bulk statistics that are no longer supported in release 15.0.
None for this release.

New NAT Output Fields and Counters
This section identifies new NAT show command output fields and counters available in release 15.0.

show active-charging analyzer statistics name sip
The following fields have been added to the output of this command:
• Total SIP Calls
• Current SIP Calls
• Total SIP UDP Calls
• Current SIP UDP Calls
• Total SIP TCP Calls
• Current SIP TCP Calls

show active-charging firewall statistics
The following fields have been added to the output of this command:
• Current Flows Processed by Firewall
• Current NAT Flows Processed by Firewall
• Current NAT44 Flows Processed by Firewall
• Current NAT64 Flows Processed by Firewall
• Current Bypass-NAT Flows Processed by Firewall
• Current Bypass-NAT44 Flows Processed by Firewall
• Current Bypass-NAT64 Flows Processed by Firewall
show active-charging firewall statistics verbose

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

- Current Flows Processed by Firewall
- Current NAT Flows Processed by Firewall
- Current NAT44 Flows Processed by Firewall
- Current NAT64 Flows Processed by Firewall
- Current Bypass-NAT Flows Processed by Firewall
- Current Bypass-NAT44 Flows Processed by Firewall
- Current Bypass-NAT64 Flows Processed by Firewall

show active-charging sessions full

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

- Firewall Policy IPv4
- Firewall Policy IPv6
- Bypass NAT Flow Present

show active-charging subsystem all

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

- SIP ALG Calls:
  - Total SIP ALG Calls
  - Current SIP ALG Calls
  - Total UDP SIP ALG Calls
  - Current UDP SIP ALG Calls
  - Total TCP SIP ALG Calls
  - Current TCP SIP ALG Calls

Modified NAT Output Fields and Counters

This section identifies modified NAT show command output fields and counters available in release 15.0.

show active-charging firewall statistics

The following fields have been modified in the output of this command:

- Total Bypass-NAT44 Flows Processed by Firewall (Total Bypass-NAT IPv4 Flows Processed by Firewall)
- Total Bypass-NAT64 Flows Processed by Firewall (Total Bypass-NAT IPv6 Flows Processed by Firewall)

show active-charging firewall statistics verbose

The following fields have been modified in the output of this command:
- Total Bypass-NAT44 Flows Processed by Firewall (Total Bypass-NAT IPv4 Flows Processed by Firewall)
- Total Bypass-NAT64 Flows Processed by Firewall (Total Bypass-NAT IPv6 Flows Processed by Firewall)

**Deprecated NAT Output Fields and Counters**

This section identifies deprecated NAT output fields and counters that are no longer supported in release 15.0.

**show active-charging firewall statistics verbose**

The following field has been deprecated:
- Packets Dropped due to No Ruledef in Rulebase

**show active-charging firewall statistics callid <call_id> verbose**

The following field has been deprecated:
- Packets Dropped due to No Ruledef in Rulebase

**show active-charging firewall statistics domainname <domain_name> verbose**

The following field has been deprecated:
- Packets Dropped due to No Ruledef in Rulebase

**show active-charging firewall statistics username <user_name> verbose**

The following field has been deprecated:
- Packets Dropped due to No Ruledef in Rulebase
Chapter 17
PDSN Changes in Release 15.0

This chapter identifies features and functionality added to, modified for, or deprecated from 15.0 PDSN software releases.

Important: Enhancements to Diameter, GTPP, and RADIUS in release 15.0 are located in the Accounting Management Changes chapter. Enhancements to SNMP MIBs in release 15.0 are located in the SNMP MIB Changes chapter. Enhancements to Web Element Manager (WEM) in release 15.0 are located in the Web Element Manager Changes chapter.
PDSN Enhancements for February 27, 2015

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

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

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

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

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

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

**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.
CSCus51341 - [L2TP] ICRQ to include IMSI based on config CLI

Feature Changes

ICRQ message for L2TP session has calling-number to be derived from IMSI.

Adding a LAC service level CLI to configure so that IMSI has the higher priority than MSISDN/MDN.

Previous Behavior: MSISDN/MDN is used for calling-number. It has higher priority than IMSI which results in the authentication failure on LNS that uses IMS for authentication.

New Behavior: On configuring the CLI, it will ensure that IMSI is used as calling number in ICRQ.

Customer Impact:

Command Changes

allow

With this release, the calling-number keyword has been introduced to ensure that IMSI is used as calling number in ICRQ always.

configure

context context_name

lac-service lac_service_name

allow calling-number value imsi

no allow calling-number

end

Important: This is a customer specific feature.

Notes:

- If this CLI is not configured, then MSISDN/MDN will be used as calling number.
PDSN Enhancements for October 31, 2014

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

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

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

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

---

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

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

---

**CSCup93612** - PDSN support for enhanced PPP Redirection

**Feature Changes**

**Support for Enhanced PPP Redirection**

Support for enhanced PPP redirection has been added, behaviour of which is as follows:

- When subscribers access PDSN from restricted PCF area, PDSN redirects subscribers to a specific PDSN.
- When subscribers handoff from restricted PCF area to unrestricted PCF area, PDSN terminates the session.
- When subscribers handoff from unrestricted PCF area to restricted PCF area, PDSN terminates the session.
- When subscribers handoff from restricted PCF area to another restricted PCF area, PDSN terminates the session.

**Important:** This is a customer specific feature.
Command Changes

enhanced-pcf-redirection

A new command `enhanced-pcf-redirection` has been added to enable or disable the PCF redirection feature.

```
configure
  context context_name
    pdsn-service pdsn_service
      [ default | no ] enhanced-pcf-redirection
    end
```

policy pcf-zone-match

The command `policy pcf-zone-match` has been modified to add PCF redirection feature.

```
configure
  context context_name
    pdsn-service pdsn_service
      policy pcf-zone-match <zone number> [redirect <addr1> [weight <weight1>] [ <addr2> [weight <weight2>]] ...] | {restricted [redirect <addr1> [weight <weight1>] [ <addr2> [weight <weight2>] ] ...]}
    end
```
PDSN Enhancements for April 10, 2014

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

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

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

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

---

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

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

---

**CSCun65435 - Assertion at sessmgr_imsa.c:453 Function: sessmgr_authorize_with_imsa()**

**Feature Changes**

**IMSA Session for Mobile-IP Call on PDSN and HA**

**Previous Behavior:** Earlier, an IMSA session was being created for mobile-ip call on PDSN and HA together.

**New Behavior:** For mobile-ip call, the IMSA session is present only on HA, while the earlier IMSA session created by PDSN is terminated. This behaviour is only for IMSA session, while it is consistent for ACS session.
PDSN Enhancements for Jan 31, 2014

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

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

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

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

---

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

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

---

**CSCud88827 - PCF-wise bulkstats & reports**

**Feature Changes**

**Generating Bulkstats and Reports PCF**

PCF has been added as an index in the PPP and RP bulk stat schemas. It is now possible to generate reports based on the following:

- **Based on Per-PCF:** This report lists KPIs for every individual PCF, which PCF is serving. So, if the PDSN is serving 1000 PCFs, this report would contain 1000 rows.

**Performance Indicator Changes**

**PPP Per PCF Schema**
PCF has been added as an index in the PPP schema. Counters that were modified with the additional PCF index are:

PPP(vpnname, vpnid, servname, svctype, PCF)
- Total Session Initiated
- Successful Session
- Successful LCP Session
- Successful Authentication sessions
- Successful IPCP Sessions

PPP Per RP Schema

PCF has been added as an index in the RP schema. Counters that were modified with the additional PCF index are:

RP(vpnname, vpnid, servname, svctype, PCF)
- Total Registration received
- Total Registration successful
- Total Registration updated
- Total Registration update acknowledged
- Total bytes received (Optional)
- Total Bytes sent (Optional)

**show ppp statistics pcf-address [ pcf_ip_addr | all ]**

The existing command has been modified to give the following output — Displays statistics only for the time the session is connected to the specified PCF (Packet Control Function) or for all PCFs. This also displays PCF wise statistics for PPP. `pcf_ip_addr` must be specified using IPv4 dotteddecimal notation.

**show bulkstats variables rp-per-pcf**
- %vpnname%
- %vpnid%
- %servname%
- %servid%
- %pcf-ip-addr%
- %recv-total%
- %accept-total%
- %update-total%
- %update-ack-reCV-total%

**show bulkstats variables ppp-per-pcf**
- %vpnname%
- %vpnid%
CSCue70505 - Add PCF as an Index in PPP and RP Schemas

Feature Changes

Add PCF as an Index in PPP and RP Schemas

WEM now supports PCF as an index in PPP and RP schemas.

Previous Behavior: PPP Per PCF Schema and PPP Per RP Schema was not supported.

New Behavior: PPP Per PCF Schema and PPP Per RP Schema is now supported.

Performance Indicator Changes

PPP Per PCF Schema

Added ppp-per-pcf schema support in WEM.

• vpname
• vpnid
• servname
• servid
• pcf-ip-addr
• recv-total
• accept-total
• update-total
• update-ack-recv-total

PPP Per RP Schema

Added ppp-per-rp schema support in WEM.

• vpname
• vpnid
- servname
- servid
- pcf-ip-addr
- total-init
- total-sess-succ
- total-sess-succ
- total-auth
- total-ipcp
PDSN Enhancements for November 30, 2013

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

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

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

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

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

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

**CSCuj49921 - IP Pool Group bulkstat variables show individual pool stats**

**Feature Changes**

**IP Pool Group Bulkstat Variables Semantics Change**

**Previous Behavior:** Bulkstat values earlier showed the individual pool's statistics, instead of the complete group's statistics.

**New Behavior:** Newly added IP pool group based bulkstat variables now show combined statistics of the group, to which the queried ip pool is a part of.

**Performance Indicator Changes**

**show bulkstats variables ippool**
The following variables will display the combined statistics of the group, to which the queried ip pool is a part of.

- `groupname-ipv4used`
- `groupname-ipv4hold`
- `groupname-ipv4rele`
- `groupname-ipv4free`
- `groupname-ipv6used`
- `groupname-ipv6hold`
- `groupname-ipv6rels`
- `groupname-ipv6free`
PDSN Enhancements for September 30, 2013

PDSN Feature Changes as of September 30, 2013

This section provides information on PDSN feature changes in release 15.0.

New PDSN Features

This section identifies new features for the PDSN available in this release.

None for this release.

Modified PDSN Features

Auto PCFReachable Alarm Clearing Requirement at WEM

Previous Behavior: Alarms were not being cleared when PCF is reachable.
New Behavior: Alarms are now being cleared when PCF is reachable as PCFReachable trap has been added.

PDSN/FA Support for Dynamic HA Assignment

Upon receiving an RRP message with successful registration indication (code 0) for the Mobile Station (MS), PDSN updates the mobility binding for the MS, which is indexed by the NAI and the Home Address (if non zero) in the RRQ, with the HA address and the Home Address from the RRP. PDSN is not required to verify the source ip address of the RRP. This is a customer specific enhancement.

Utilization Reports Fetched for IP Pool Groups

You can now fetch reports based on the IP pool group name without errors.

PDSN/HA Combo Qualification on ASR5500

PDSN+HA combo is now supported on ASR5500.

PDSN Command Changes as of September 30, 2013

This section provides information on PDSN command changes in release 15.0.

None for this release.

PDSN Performance Indicator Changes as of September 30, 2013

This section provides information on PDSN performance indicator changes in release 15.0.

None for this release.
Chapter 18
P-GW Changes in Release 15.0

This chapter identifies features and functionality added to, modified for, or deprecated from 15.0 P-GW software releases.


The following points to changes made in this document to correct omissions or technical errors made in the previously published Release Change Reference. In content for:

- September 30, 2013:
  - GTP Throttling corrected in New P-GW Features,
  - Overcharging Protection Support corrected in New P-GW Features,
  - egtp overcharge-protection command description corrected in Modified Commands,
  - new bulk statistics added in New in the P-GW Schema section,
  - corrected descriptions and output content for New P-GW Output Fields and Counters:
    - show apn statistics all
    - show pgw-service all
    - show pgw-service statistics all
    - show subscribers full
    - show subscribers pgw-only full all
    - show subscribers summary
P-GW Enhancements for February 27, 2015

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 *Packet Data Network Gateway 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
- GTPPP Enhancements
- Lawful Intercept Enhancements
- MVG Enhancements
- NAT Enhancements
- SNMP MIB Enhancements
- System and Platform Enhancements

---

**CSCuc76443 - Wrong IE in PDP response to PDP context without TFT already activated**

**Feature Changes**

**CPC Reject Reason**

**Previous Behavior:** A Packet Data Protocol (PDP) Context existed without an associated Traffic flow template (TFT) for a given Packet Data Network (PDN). After receiving a Create PDP context request without a Traffic flow Template, the GGSN sent a Create PDP context response with the cause code 199 "No resources available".

**New Behavior:** Now, if a Packet Data Protocol Context exists without any associated Traffic flow template for a given Packet Data Network, then the GGSN will send a Create PDP context response with the cause code 221 "PDP context without TFT already activated" for a Create PDP context request without a Traffic flow Template.
P-GW Enhancements for October 31, 2014

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 *Packet Data Network Gateway 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

---

**CSCui10427 - default behavior for vrf-multipath is to use the global multipath**

**Feature Changes**

**Default Behavior for vrf-multipath is to Use Global Multipath**

**Previous Behavior:** There was an error where the multipath configured under “address-family ipv4 vrf <>” was never being used. The multipath value under the router bgp level was being used instead.

**New Behavior:** If the multipath is configured under vrf mode, then this value is used for prefixes under vrf. If multipath is not configured under vrf-mode, then the router bgp multipath values are used for prefixes in the vrf.

**Customer Impact:** If the customer was not using any config under the vrf-mode then there is no difference. If the customer was using the multipath value under the vrf-mode, then the difference is that this config will start taking affect.
CSCuo06912 - PGW call fails if Framed-Pool enforced from radius

Feature Changes

P-GW Call Fails if Frame-Pool Enforced from Radius

In P-GW, if radius returned ip pool in access accept, then this scenario was not handled correctly.

Previous Behavior: For P-GW, if radius returned ip pool for ip address alloc method as no-dynamic, then ip address allocation was not successful.

New Behavior: For P-GW, if radius returns ip pool for ip address alloc method as no-dynamic, then ip address allocation will be successful.

Customer Impact: The customer will be able to use no-dynamic ip alloc method for radius returned ip pool.

CSCuo95038 - PGW forces lower AMBR values than received

Feature Changes

P-GW forces lower AMBR values than received

Previous Behavior: In absence of PCRF, the APN AMBR that was received in the MOB BEARER REQUEST during GnGp HO was not applied.

New Behavior: In absence of PCRF, the APN AMBR received in MOB BEARER REQUEST during GnGp HO will now be applied.

CSCuq39165 - [OCS FOA] Create Session Response is not sent out from PGW

Feature Changes

Create Session Response is Not Sent Out From P-GW

Previous Behavior: In an LTE new call, the call failed with a CS Response ‘NO_RESOURCEAVAILABLE’ if the PAP/CHAP parameters were absent in the CS Request message and the PAP/CHAP auth was configured as mandatory in the boxeq config.

New Behavior: A call now fails with the CS Response ‘USER_AUTHENTICATION_FAILED’.
P-GW Enhancements for January 31, 2014

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 *Packet Data Network Gateway 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

---

**CSCug69032 - if v6 pcscf address is not available, ip name-server addresses are sent**

**Feature Changes**

**P-CSCF Discovery**

P-GW will not return IP name server address if P-CSCF address is requested.

**Previous Behavior:** After DNS query (query on FQDN that P-GW receives on S6b) is performed, P-GW can get up to three addresses in pcscf_ip_addr[]. These addresses are encoded in PCO IE. If from here the P-GW does not get any address in pcscf_ip_addr, then it looks for other options.

Priority of addresses is as follows:

1. Addresses from S6b.
2. Addresses from Radius or configured in APN.
3. Addresses configured in the destination context.

**New Behavior:** After DNS query (query on FQDN that P-GW receives on S6b) is performed, system can get up to three addresses in pcscf_ip_addr[]. These addresses are encoded in PCO IE. If from here the P-GW does not get any address in pcscf_ip_addr, then it looks for other options.

Priority of addresses is now as follows:

1. Addresses from S6b.
2. Addresses from Radius or configured in APN.
The third case, where address was returned from destination context configuration, has been removed.

**CSCuh28006, CSCul24601 - Additional application support with DSCP-802.1p Marking per Interface**

**Feature Changes**

**Internal-QoS**

To consolidate L2-level QoS marking across all interfaces, marking IP-DSCP values will be left to individual applications as applications build IP headers. The DSCP value in IP-header will then be used to derive the L2 QoS Values by platform (NPU). This derivation will be done in two steps.

1. DSCP will be mapped to an Internal-QoS value using a system-wide table.
2. Internal-QoS will be mapped to actual L2 value (either or both of 802.1p/MPLS) using a per-vrf based table.

Internal-QoS (Internal-Per-Hop-Behavior/IPHB) consists of 5 bits. 3 bits of class-of-service is user-configurable, while the remaining 2 bits are left for future use to dynamically stamp a drop eligibility based on a rate-monitor.

The 64 DSCP values will map, each to any of the available 8 COS values of Internal-QoS. The 5 bits of Internal-QoS will then map to 3+1 bits of 802.1p (the tos and drop-eligibility-indicator) and 3 bits of MPLS-Traffic-Class.

**Command Changes**

**qos ip-dscp-iphb-mapping**

This new command is used to manage Internal QoS (Internal-Per-Hop-Behavior/IPHB). This specific command maps IP Differentiated Services Code Point (DSCP) values in a packet to internal-QoS class of service marking values.

```
configure

qos ip-dscp-iphb-mapping dscp dscp_value internal-priority cos class_of_service_value

[ default | no ] qos ip-dscp-iphb-mapping dscp dscp_value

end
```

**qos 12-mapping-table**

This new command is used to create or modify an L2 mapping table, which is used to map internal values to L2 values like 802.1p and MLPS.

```
configure
```
Changes in Release 15.0

GW Enhancements for January 31, 2014

[ no ] qos l2-mapping-table [ name map_table_name | system-default ]
end

internal-priority

This new command is used to map internal QoS priority with Class of Service (COS) values.

configure

qos l2-mapping-table name map_table_name

[ default ] internal-priority cos cos_value color color_value 802.1p-value 802.1p-value mpls-tc mpls-tc-value
end

associate

This new command is used to associate an internal QoS L2 mapping table to a VPN context.

configure

context vpn_name

associate 12-mapping-table [ name l2_mapping_table_name | system-default ]

[ default ] associate l2-mapping-table
end

Notes:

- If an l2-mapping-table association is made at both the VRF and VPN level, the VFR level takes precedence.
- If no explicit association is created/configured, the system-default mapping table is used.

associate

This new command is used to associate an internal QoS L2 mapping table to a specific VPN Routing and Forwarding (VRF).

configure

context vpn_name

ip vrf vrf_name

associate 12-mapping-table [ name l2_mapping_table_name | system-default ]

[ no ] associate l2-mapping-table
end

Notes:

- If an l2-mapping-table association is made at both the VRF and VPN level, the VFR level takes precedence.
• If no explicit association is created/configured, the system-default mapping table is used.

Performance Indicator Changes

show qos ip-dscp-iphb-mapping

This new command displays mapping qos information in a packet to internal-qos marking.

show qos l2-mapping-table system-default

This new command displays system default internal mapping to l2 values, like 802.1p and mpls.

show qos l2-mapping-table name table_name

This new command displays named table for the internal to l2 mapping values, like 802.1p and mpls.

CSCuj91396 - egtpmgr 143137 info GTP-C path failure egtpmgr on Standby

Feature Changes

GTP-C Path Failure

Time required to detect path failure for first time after restart is increased to 180 seconds (considering default values for gtpc echo interval as 60 and gtpc retransmission-timeout as 5).

Previous Behavior: After restart, eGTP used to detect path failure after 80 seconds.

New Behavior: The time required to detect path failure for the first time after restart is increased to 180 seconds. This will allow sessmgr to come up and report the SRP state to eGTPC. Considering the default values for gtpc echo interval as 60 and gtpc retransmission-timeout as 5, the number of retries for first echo have been changed to 24, which would effectively mean that path failure will be detected after 180 seconds.

If the values of gtpc echo interval and/or gtpc retransmission-timeout are changed, the time will vary according to the following logic.

\[(gtpc\ echo\ interval + (gtpc\ retransmission-timeout\ X\ gtpc\ max-retransmissions))\]

\[60 + 5 \times 24 = 180\]

For the first echo, the configured value of gtpc max-retransmissions will be ignored and assumed to be “24”. After the first successful echo, eGTPC will fallback to configured value of gtpc max-retransmissions, either in peer-profile or egtp-service configuration, whichever holds precedence.

CSCul24817 - Change in the 802.1p/MPLS-EXP configuration in QCI table

Feature Changes

QoS Mapping
The explicit configuration of 802.1p/MPLS-EXP is being deprecated and it will be replaced by new construct of internal-qos.

**Previous Behavior:** Operator can set 802.1p and mpls priorities in the `qci-qos-mapping` table.

**New Behavior:** Operator can only configure internal-qos parameters.

**Customer Impact:** Due to backward compatibility, previous configuration should still work.

Going forward, customer can only configure `internal-qos` in `qci-qos-mapping` table.

**Command Changes**

`qci`

Keywords `802.1p-value` and `mpls-exp-value` have been deprecated. The values provided using these deprecated keywords will be mapped to new `internal-qos` values.

`configure`

```
qci-qos-mapping name

qci num uplink { encaps-header | internal-qos priority priority | user-datagram }
downlink { encaps-header | internal-qos priority priority | user-datagram }

[ default | no ] qci num

end
```

Notes:
- `internal-qos`: Set the internal QoS priority where priority is an integer from 0-7, where 7 is the highest priority and 0 is the lowest priority; These are resolved to L2 values.

**Performance Indicator Changes**

`show apn statistics`

“802.1p” removed from “802.1p Priority Marking Statistics” field.

`show pgw-service statistics all`

“802.1p” removed from “802.1p Priority Marking Statistics” field.

`show qci-qos-mapping table all`

Output similar to the following is now shown for internal QoS:
- uplink: internal-qos priority 5
- downlink: internal-qos priority 3

`show sgw-service statistics all`

“802.1p” removed from “802.1p Priority Marking Statistics” field.
**CSCul65556 - Sessmgr Crashes on seeing dhcpv6 server statistics**

**Feature Changes**

**DHCPv6 Server Statistics**

*Previous Behavior:* When checking DHCPv6 server statistics, Session Manager crashed and all existing DHCPv6 and PD calls were released.

*New Behavior:* Obsolete CLIs that led to the Session Manager crash have been removed.

*Customer Impact:* Obsolete CLIs were not giving any relevant information.

**Performance Indicator Changes**

*show dhcpv6*

The keyword `server` option has been removed.

*show dhcpv6 counters*

The keyword `server` option has been removed.

*show dhcpv6 full*

The keyword `server` option has been removed.

*show dhcpv6 statistics*

The keyword `server` option has been removed.

*show dhcpv6 summary*

The keyword `server` option has been removed.

**CSCul93209 - Need show config errors to point inconsistencies in qos configuration**

**Performance Indicator Changes**

*show configuration errors section qos-marking verbose*

A new section is added in `show configuration errors` to capture related to QoS configuration introduced as part of CSCuh28006.

---

**Important:** The new section is only available in `verbose` option.

A sample output of the new section, along with the new errors/warnings, is shown below:
Error: VPN context vpn1 has a qos table association vpn1table, that does not exist!

Error: VPN context vpn1, vrf vrf1 has a qos table association vrf1table, that does not exist!

Error: Qos Table test-table has no associations from any vpn/vrf

Total 3 error(s) in this section!

Warning: 12 tables system-default and test-table2 have the same mapping. This is redundant.

Warning: VPN context vpn1 and vrf vrf2 have the same association vpn1table. The vrf association is redundant.

Total 2 warning(s) in this section!
P-GW Enhancements for November 30, 2013

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 *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 P-GW.

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

---

**CSCuf65085 - CxGW:Wrong update of ULI to PCRF during idle tau w/o mme/sgw relocation**

**Feature Changes**

**ULI Change Trigger and CLI Output in Some Error Conditions**

**Previous Behavior:** Initially, system receives TAI and ECGI in ULI. If an error condition triggered an update with same ECGI value, system updated ULI with duplicate value and sent ULI change trigger to IMSA, even though there was no change in ECGI.

**New Behavior:** Initially, system receives TAI and ECGI in ULI. If an error condition triggers an update with same ECGI value, system no longer updates ULI and does not send ULI change trigger to IMSA since there is no change in ECGI.

**Customer Impact:** None.
CSCuf80818 - Enhancement to have the delta route modifier for SRP systems ASR5X

Feature Changes

Delta Route Modifier for SRP Systems

In HA/HAGR design, the Active and Standby systems have route modifier delta of “1”. Network design requires Active/ICSR to be able to advertise with a delta modifier that is configurable.

Command Changes

delta-route-modifier

Specifies the delta that will be used to compute the route modifier difference between the active and standby chassis. Prior to this release, the delta is applied only in the standby state. For this release, it is used in both states.

configure

    configure context ctx_name
    service-redundancy-protocol
    delta-route-modifier value
    end

CSCuh66364 - Acct-Termination-Cause in acct stop msg shows Unknown SRVCC PS to CS HO

Feature Changes

Rf Interface and Radius Accounting Interface

Previous Behavior: In case of SRVCC PS to CS handover, in accounting stop record message, Acct-Termination-Cause for RADIUS accounting and termination-cause for Rf interface is sent as Unknown.

New Behavior: In case of SRVCC PS to CS handover, in accounting stop record message, Acct-Termination-Cause for RADIUS accounting and termination-cause for Rf interface will be sent as NAS_request since handover will be triggered by eNodeB.
CSCuh71681 - END_USER_IMSI value received on S6b is reported as END_USER_E164 on Gy, Rf

Feature Changes

IMSI Received on PBU Reported in Both Gy and Rf Accounting Messages

**Previous Behavior:** For P-GW, the IMSI value received in S6b AAA was being reported in Rf accounting messages and IMSI received on PBU was reported on Gy accounting messages.

**New Behavior:** For P-GW, the IMSI value received in S6b AAA is ignored and IMSI received on PBU is reported in both Gy and Rf accounting messages.

**Customer Impact:** None.

CSCuh73686, CSCul49747 - P-GW: Modification of ‘timeout bearer-inactivity’ CLI to ignore default bearer

Feature Changes

Timeout Bearer Inactivity Feature

**Previous Behavior:** The timeout bearer-inactivity CLI monitored all bearers on the PDN for inactivity. If the default bearer timed out unexpectedly, it caused the session to be torn down and the user was disconnected. This feature also looked at both uplink and downlink data.

**New Behavior:** The bearer inactivity timer can now be configured to exclude default bearer/primary bearer from monitoring bearer inactivity. In addition, this feature now has the option to look at either uplink or downlink data.

Command Changes

```
timeout bearer-inactivity
```

This command configures the bearer inactivity timer and the threshold value of the traffic through an APN.

New keywords have been added so the threshold value can now be configured for monitoring traffic at various levels. The bearer inactivity timer can also be configured to exclude default bearer/primary bearer from monitoring bearer inactivity.

```
config

context context_name

apn apn_name

  timeout bearer-inactivity seconds volume-threshold { downlink bytes | total bytes | uplink bytes }

  timeout bearer-inactivity exclude-default-bearer
```
[ default | no ] timeout bearer-inactivity

end

Notes:
- Only one threshold is allowed to be configured per APN which is to monitor total, uplink, or downlink traffic.
- Bearer inactivity timer is started only when time and volume threshold is configured.
- seconds must be an integer from 900 to 2592000. The minimum configurable value of bearer inactivity timer is reduced from 3600 seconds to 900 seconds.
- volume-threshold downlink: Threshold value of the downlink data traffic in a bearer.
- volume-threshold total: Threshold value of the uplink and downlink data traffic in a bearer.
- volume-threshold uplink: Threshold value of the uplink data traffic in a bearer.
- exclude-default-bearer: Ignore bearer inactivity handling for default/primary bearer.
- default | no: The bearer inactivity timer is disabled.

CSCui42540 - P-GW: DHCPv6 default UE prefix should be allocated from AAA and PD from DHCPv6

Feature Changes

DHCPv6 Default UE Prefix Allocated from AAA and PD from DHCPv6

Previous Behavior: Current implementation supports allocation of both default UE prefix and delegated prefixes from external DHCPv6 server.

New Behavior: Added support for allocating default UE prefix from local/AAA and delegated prefix from external DHCPv6 server.

CSCui47287 - AAA radius returned ip address should be dynamic for PGW

Feature Changes

RADIUS/S6b Returned IP Address Dynamic for P-GW

Previous Behavior: For P-GW, system considered RADIUS assigned IP address as Static. For GGSN, system considered both RADIUS and S6b assigned IP addresses as Static.

New Behavior: With new implementation, system now considers both RADIUS and S6b assigned IP address as Dynamic at P-GW and GGSN.

Customer Impact: The DynAddressFlag AVP, which is sent to P-GW and GGSN CDRs, will now contain value as Dynamic if IP address is assigned from RADIUS or S6b.
CSCui98507 - Call loss when SGW restoration with same SGW in progress

Feature Changes

GTP-U Management Changes During S-GW Restoration

Previous Behavior: GTPUMGR sessions were not cleaned up on moving to S-GW Restoration State and GTP-U ECHO continued to happen and stopped only after GTP-U PATH failure detection. Error Indication was honored as normal.

New Behavior: On entering S-GW Restoration state, GTPUMGR session entries will be cleaned up and it will stop GTP-U ECHO towards peer S-GW. GTP-U session entries will rebuild on receiving MBReq to recover the sessions. GTPUMGR will drop ERROR_IND if the session is in S-GW Restoration State.

Customer Impact: If S-GW follows recommendation from 23.007, then no subscriber impact. If S-GW does not follow, then during S-GW restoration, 50% or more calls could be lost.

CSCul23543 - PGW rejects session with Status as Adminiprohibited in PMIP PBA

Feature Changes

Starent-Subscriber-Permission AVP Validation

Previous Behavior: LMA/PMIP P-GW calls rejected if Starent-Subscriber-Permission AVP if received from S6b and 0x04 bit is not set.

New Behavior: Validation of Starent-Subscriber-Permission AVP not done for LMA/PMIP P-GW calls so behavior is consistent with LTE calls and calls are not rejected.
P-GW Enhancements for October 30, 2013

P-GW Feature Changes as of October 30, 2013

This section provides information on P-GW feature changes in release 15.0.

**Important:** For more information regarding features in this section, refer to the *P-GW Administration Guide* for this release.

New P-GW Features

This section identifies new P-GW features available in release 15.0.

None for this release.

Modified P-GW Features

This section identifies P-GW features modified in release 15.0.

**Improved Session Management During S-GW Restoration**

**Previous Behavior:** During S-GW Restoration, when the S-GW has recovered and starts reusing same TEID range for GTPU sessions prior to restart, the S-GW did not properly clear GTPUMGR sessions and GTPU ECHO messages continued to be sent.

**New Behavior:** When entering the S-GW Restoration State, GTPUMGR session entries are now cleared and the S-GW will stop GTPU ECHO messages towards the peer S-GW.

GTPU session entities will be re-built upon receiving a MBReq to recover the sessions.

GTPUMGR will drop ERROR_IND if the session is in S-GW Restoration State.

P-GW Command Changes as of October 30, 2013

This section provides information on P-GW command changes in release 15.0.

None for this release.

P-GW Performance Indicator Changes as of October 30, 2013

This section provides information on P-GW performance indicator changes in release 15.0.

None for this release.
P-GW Enhancements for September 30, 2013

P-GW Feature Changes as of September 30, 2013

This section provides information on P-GW feature changes in release 15.0.

**Important:** For more information regarding features in this section, refer to the *P-GW Administration Guide* for this release.

New P-GW Features

This section identifies new P-GW features available in release 15.0.

**Authorized Qos Policy to be Displayed at SM for P-GW and SAEGW**

Code added to display PCRF authorized in `show subscribers pgw-only full all` for P-GW and in `show subscribers saegw-only full all` for SAEGW.

**eGTP-C Support for Enhanced S-GW Restoration**

This functionality is now supported. See *S-GW Restoration Support on P-GW* for more information.

**GTP Throttling**

**Corrected Content:** This section includes corrections to previously published content. The previous content stated that, “This feature has been implemented as lab quality. All associated CLI commands and performance statistics are also now supported at lab quality”, which is incorrect. GTP Throttling functionality has been implemented as deploy quality.

This feature will help control the rate of incoming/outgoing messages on P-GW/GGSN. This will help in ensuring P-GW/GGSN doesn’t get overwhelmed by the GTP control plan messages. In addition, it will help in ensuring the P-GW/GGSN will not overwhelm the peer GTP-C peer with GTP Control plane messages.

**Important:** Use of GTP and Diameter Interface Throttling requires that a valid license key be installed. Contact your Cisco account representative for information on how to obtain a license.

This feature requires shaping/policing of GTP (v1 and v2) control messages over Gn/Gp and S5/S8 interfaces. Feature will cover overload protection of P-GW/GGSN nodes and other external nodes with which it communicates.

**Important:** GTP throttling will be done only for session level control messages. Path management messages will not be rate limited.

External node overload can happen in a scenario where P-GW/GGSN generates signaling requests at a higher rate than other nodes can handle. Also, if the incoming rate is high at P-GW/GGSN node, we might flood any of the external nodes; hence, throttling of both incoming and outgoing control messages is required.
For protecting external nodes from getting overloaded from P-GW/GGSN control signaling, a framework will be used to handle shaping/policing of outbound control messages to external interfaces.

**GTP-U Support for Enhanced S-GW Restoration**

This functionality is now supported. See [S-GW Restoration Support on P-GW](#) for more information.

**License Enforcement for Overcharging Protection Feature in P-GW**

New license key introduced for Overcharging Protection for P-GW functionality.

<table>
<thead>
<tr>
<th>Important:</th>
<th>Contact your Cisco account representative for information on how to obtain a license.</th>
</tr>
</thead>
</table>

**License for Enhanced S-GW Restoration**

No additional license key is required for the S-GW Restoration functionality; it is included in the P-GW session use license.

**License Enforcement for NEMO Support in GGSN**

New license key introduced for Dynamic Network Mobile Routing (NEMO) for GGSN functionality.

<table>
<thead>
<tr>
<th>Important:</th>
<th>Contact your Cisco account representative for information on how to obtain a license.</th>
</tr>
</thead>
</table>

**License Enforcement for GTP Throttling**

New license key introduced for Rate Limiting Function (Throttling) functionality.

<table>
<thead>
<tr>
<th>Important:</th>
<th>Contact your Cisco account representative for information on how to obtain a license.</th>
</tr>
</thead>
</table>

**License Enforcement for IPNE**

New license key introduced for Intelligent Programmable Network Element (IPNE) support.

<table>
<thead>
<tr>
<th>Important:</th>
<th>Contact your Cisco account representative for information on how to obtain a license.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Important:</th>
<th>IPNE functionality has been implemented as lab quality.</th>
</tr>
</thead>
</table>

**MINE/IPNE Support**

The P-GW in the ASR 5x00 provides user, device, and session information to the MINE framework via XMPP.

<table>
<thead>
<tr>
<th>Important:</th>
<th>This functionality has been implemented as lab quality.</th>
</tr>
</thead>
</table>

**MPLS EXP Marking of User Plane Traffic**
Similar to 802.1p marking, MPLS EXP bit marking is supported for Enterprise APN’s that use MPLS tunneling on the SGi interface on the P-GW. The QoS marking used in the LTE/EPC network (QCI per EPS bearer) is mapped to the 802.1p and MPLS EXP bit marking between the P-GW and L2/EPC switch and MPLS/PE routers (this is applicable to the upstream direction, from the P-GW to the Network). MPLS EXP marking related configuration is available as part of the QCI-QOS configuration table. MPLS EXP marking is selected based on QCI of the bearer to which that packet belongs.

**MTU Size PCO**

UEs usually use a hardcoded MTU size for IP communication. If this hardcoded value is not in sync with the network supported value, it can lead to unnecessary fragmentation of packets sent by the UE. Thus, in order to avoid unnecessary fragmentation, this feature helps in using the network-provided MTU size instead of the hardcoded MTU in UE.

3GPP defined a new PCO option in Release 10 specifications for the network to be able to provide an IPv4 MTU size to the UE. P-GW will support an option to configure a IPv4 Link MTU size in the APN profile.

If the UE requests IPv4 Link MTU size in the PCO options during Initial Attach or PDN connectivity request, the P-GW will provide the preconfigured value based on the APN.

If the MTU size configuration on APN is changed, the new MTU size will take effect only for new PDN connections and initial attaches. P-GW will not update for the existing PDN connections.

If UE does not request IPv4 Link MTU size, P-GW will not include the IPv4 Link MTU size.

**Multi-VRF Support Over NEMO**

**Previous Behavior:**
- MR device may be used for multiple VRFs to connect within different enterprise networks.
- HA service shall enable the MR to work with independent enterprise networks.

**New Behavior:**
- Each enterprise network is associated with its own VRF. Both MR and HA share common vrf-names.
- MR and HA services are enhanced to support Cisco NVSE extension for NEMO with multiple VRF.

**Node Functionality GTP Echo**

This feature helps exchange capabilities of two communicating GTP nodes, and uses the new feature based on whether it is supported by the other node.

This feature allows S-GW to exchange its capabilities (MABR, PRN, NTSR) with the peer entities through ECHO messages. By this, if both the peer nodes support some common features, then they can make use of new messages to communicate with each other.

With new “node features” IE support in ECHO request/response message, each node can send its supported features (MABR, PRN, NTSR). This way, S-GW can learn the peer node’s supported features. S-GW’s supported features can be configured by having some configuration at the service level.

If S-GW wants to use new message, such as P-GW Restart Notification, then S-GW should check if the peer node supports this new feature or not. If the peer does not support it, then S-GW should fall back to old behavior.

If S-GW receives a new message from the peer node, and if S-GW does not support this new message, then S-GW should ignore it. If S-GW supports the particular feature, then it should handle the new message as per the specification.

**Overcharging Protection Support**
Corrected Content: This section includes corrections to previously published content. The previous content stated that, “Overcharging Protection functionality has been implemented as lab quality”, which is incorrect. Overcharging Protection functionality has been implemented as deploy quality.

Overcharging Protection helps in avoiding charging the subscribers for dropped downlink packets while the UE is in idle mode. In some countries, it is a regulatory requirement to avoid such overcharging, so it becomes a mandatory feature for operators in such countries. Overall, this feature helps ensure subscriber are not overcharged while the subscriber is in idle mode.

Important: Use of Overcharging Protection in P-GW requires that a valid license key be installed. Contact your Cisco account representative for information on how to obtain a license.

P-GW will never be aware of UE state (idle or connected mode). Charging for downlink data is applicable at P-GW, even when UE is in idle mode. Downlink data for UE may be dropped at S-GW when UE is in idle mode due to buffer overflow or delay in paging. Thus, P-GW will charge the subscriber for the dropped packets, which isn’t desired. To address this problem, with Overcharging Protection feature enabled, S-GW will inform P-GW to stop or resume charging based on packets dropped at S-GW and transition of UE from idle to active state.

Once the criterion to signal “stop charging” is met, S-GW will send Modify Bearer Request (MBReq) to P-GW. MBReq would be sent for the PDN to specify which packets will be dropped at S-GW. MBReq will have a new private extension IE to send “stop charging” and “start charging” indication to P-GW.

When the MBReq with stop charging is received from a S-GW for a PDN, P-GW will stop charging for downlink packets but will continue sending the packets to S-GW.

P-GW will resume sending downlink packets after receiving “stop charging” request when either of these conditions is met:

- When the S-GW (which had earlier sent “stop charging” in MBReq) sends “start charging” in MBReq.
- When the S-GW changes (which indicates that maybe UE has relocated to new S-GW).

**Peer GTP Node Profile Configuration Support**

Provides flexibility to the operators to have different configuration for GTP-C and Lawful Intercept, based on the type of peer or the IP address of the peer.

Peer profile feature allows flexible profile based configuration to accommodate growing requirements of customizable parameters with default values and actions for peer nodes of P-GW. With this feature, configuration of GTP-C parameters and disabling/enabling of Lawful Intercept per MCC/MNC or IP address based on rules defined.

A new framework of peer-profile and peer-map is introduced. Peer-profile configuration captures the GTP-C specific configuration and/or Lawful Intercept enable/disable configuration. GTP-C configuration covers GTP-C retransmission (maximum number of retries and retransmission timeout) and GTP echo configuration. Peer-map configuration matches the peer-profile to be applied to a particular criteria. Peer-map supports criteria like MCC/MNC (PLMN-ID) of the peer or IP-address of the peer. Peer-map can then be associated with P-GW service.

Intent of this feature is to provide flexibility to operators to configure a profile which can be applied to a specific set of peers. For example, have a different retransmission timeout for foreign peers as compared to home peers.

**Per Enterprise NEMO Min Re-registration Timer Limit**

Support has been added for min-reg-lifetime at APN for 4G scenario.

If a provider offers primary LTE connection with NEMO routing, they can offer their customers a secondary carrier service for backup. This requires re-routing of traffic symmetrically to the alternate carrier in a timely manner upon a failure on the primary communication path.
**Previous Behavior:** APN configuration did not include the mobile-ip min-reg-lifetime configuration.

**New Behavior:** CLI has been added to APN for mobile-ip min-reg-lifetime to configure a platform-wide NEMO minimum registration timer to override the platform-wide default on an enterprise basis.

min-reg-lifetime taken from APN configuration if provisioned; otherwise, it will be taken from the HA service configuration.

**P-GW PMIPv6 Heartbeat**

Proxy Mobile IPv6 (PMIPv6) is a network-based mobility management protocol to provide mobility without requiring the participation of the mobile node in any PMIPv6 mobility related signaling. The core functional entities Mobile Access Gateway (MAG) and the Local Mobility Anchor (LMA) set up tunnels dynamically to manage mobility for a mobile node.

Path management mechanism through Heartbeat messages between the MAG and LMA is important to know the reachability of the peers, to detect failures, quickly inform peers in the event of a recovery from node failures, and allow a peer to take appropriate action.

Per RFC 5847, PMIP heartbeats from the HSGW to the P-GW are now supported. CLI has been added to configure the heartbeat variables. Show commands have also been modified to display the heartbeat configuration and the statistics.

**Provide Dynamic Address Flag Extension from P-GW SM**

When PAA contained single IP address for dual stack, P-GW SM was using the same macro for updating dyn_addr_flag and dyn_ipv6_addr_flag, and used the same value for both flags. This has been corrected by introducing a new macro for IPv6 addr.

**Provide dyn_ipv6_addr_flag**

Code added to provide dyn_ipv6_addr_flag value to ECS.

**S-GW Restoration Support on P-GW**

S-GW Restoration helps in handling the S-GW failure in the EPC network in a graceful manner. It allows affected PDNs due to S-GW failure to be restored by selecting another S-GW to serve the affected PDNs, thus avoiding unnecessary flooding of signaling for PDN cleanup.

S-GW Restoration is based on 3GPP Release 11. It requires enhancements at P-GW for maintaining the sessions in case path failure is detected or when S-GW restart is detected via recovery IE on GTP-C signaling. P-GW shall ensure that any dropped packets in this scenario are not charged and P-GW shall reject any bearer addition/modification request received for the PDN connection maintained after the S-GW failure detection, till the time that PDN is restored again.

Once the session has been restored by the MME (i.e., P-GW receives a Modify Bearer Request from the restarted S-GW or a different S-GW), P-GW shall resume forwarding any received downlink data and start charging them.

When subscriber is in S-GW restoration phase, all RARs (expect for Session Termination) will be rejected by PCEF. P-GW will reject all internal updates which can trigger CCR-U towards PCRF. P-GW shall trigger a CCR U with ANG-W-Change for the PDNs that are restored if the S-GW has changed on restoration.

**Important:** Only MME/S4-SGSN triggered S-GW restoration procedure will be supported. S-GW restoration detection based on GTP-U path failure shall not be considered for this release. GTP-C path failure detection should be enabled for enabling this feature.
MME/S4-SGSN shall be locally configured to know that P-GW in the same PLMN supports the S-GW restoration feature. When this feature is enabled at P-GW, it shall support it for all S-GWs/MMEs.

Unauthenticated IMSI for SM

Code changes added to send Unauthenticated IMSI flag along with emergency session type in Create request to ACS.

Modified P-GW Features

This section identifies P-GW features modified in release 15.0.

3GPP Tracing to Increase Number of Simultaneous Traces from 30 to 1000

Increases the number of simultaneous session traces that can be enabled.

**Previous Behavior:** 3GPP trace limit was 30 sessions.

**New Behavior:** 3GPP tracing has been enhanced to increase the number of simultaneous traces from 30 to 1000. The generated trace files are forwarded to external trace collection entity at regular intervals through (S)FTP if “push” mode is enabled. If the push mode is not used, the files are stored on the local hard drive and must be pulled off by the TCE using FTP or SFTP.

**Important:** The number of session trace files generated would be limited by the total available hard disk capacity.

3GPP Tracing to Intercept Random Subscriber

**Previous Behavior:** Previously, a subscriber identifier like IMSI was required in order to enable trace. Sometimes operators want to enable a trace without knowing the subscriber ID. For example, an operator may want to monitor the next “n” number of calls, or monitor subscribers in a particular IMSI range. The InTracer tool allows these use cases.

**New Behavior:** 3GPP tracing has been enhanced to intercept random subscribers with this feature. The current session trace feature is either signaling or management based, which is very specific to a particular subscriber. The requirement is to trace random subscribers which are not explicitly linked or identified by IMSI in GTP messages or configured through CLI.

The random subscribers could be in an IMSI range, context activation in particular time intervals, etc.

The session trace is activated on demand for a limited period of time for specific analysis purposes. The maximum limit would restrict the number of random subscriber tracing. Random session trace will be given priority over signalling and management-based session trace.

3GPP TS 29.281 (GTP-U) Release 10 Compliance

**Previous Behavior:** P-GW was not fully compliant to 3GPP TS 29.281 Release 10 to support UDP Port Extension header in Error indication message and Supported Extension Headers Notification message.

**New Behavior:** This feature enhances the GTP-U capabilities of P-GW in compliance to 3GPP TS 29.281 Rel-10. Support for UDP Port Extension Header in Error Indication message and Supported Extension Headers Notification message was added to become fully compliant with 3GPP Release 10.

Supported Extension Headers Notification message indicates a list of supported extension headers that the node can support. This message is sent only in case a GTP entity was required to interpret a mandatory extension header (by setting the comprehension required in extension header), but the GTP entity was not yet upgraded to support that extension header.
If a Supported Extension Headers Notification is received from peer GTP-U entity, node will not send the extension header to the peer entity.

If a message which contains extension header is received from peer GTP-U entity and the extension header is set to comprehension required and the extension header cannot be interpreted by the node, it will send a Supported Extension Headers Notification message. This message shall include all the extension headers supported by the node.

UDP Port Extension header helps in handling the Error-Indication message efficiently. If any GTP-U peer supports this extension header, then sending this extension header in Error-Indication message will help in processing the Error-Indication message.

Support for Supported Extension Headers Notification message helps notify the GTP-U peer about the GTP-U capabilities of the node. This message is sent only in case the node was required to interpret a mandatory extension header (by setting the comprehension required in extension header), but the node was not yet upgraded to support that extension header.

### 3GPP TS 32.251 Release 10 Dec 2011 Compliance

The following are now supported from 3GPP TS 32.251 Release 10:

**IMEI not known cause**

When the UE is UICCless and emergency attached, there is no valid IMSI. Therefore, it is not possible to provide the IMSI in the related messages, such as Change Notification Request message. In this case, the IMEI is included in these messages. If the IMEI is not known in the target side, the correct cause should be returned to the source side.

**IP Address Parameter**

The static address flag is sent from P-GW in the TAU/RAU/Handover with S-GW change procedure. Two flags are added in the indication.

### 3GPP Rel 11 Upgrade

The following CRs are now supported from Rel 11:

**CR-1075:** PCO

- Activate dedicated EPS bearer context accept is the NAS message used between the UE and the MME; it is not applicable for SGSN.

  After receiving the PCO sent from the SGSN/MME, S-GW shall forward it to the P-GW in the Update Bearer Response and Delete Bearer Response.

  Code changed to send PCO in Update Bearer Response and Delete Bearer Response.

**CR-1187:** Network provided Location Information

- Added new flag “RetLoc” in Indication IE
- Added Indication IE in UBReq msg
- ULI is now CO on s5 in CSReq

**CR-1194:** Usage of TEID0

- Reject response on 0 teid will not be treated as error

**CR-1197:** Additions for CS to PS SRVCC

- Added “CPSR” flag in Indication IE

**CR-1202:** Clarify mandatory/conditional IE inclusion in error response msg
• Cause inside Bearer Context in response messages will only be validated if Message level cause is accepted
   The code is currently dependent on availability of the Bearer Context and refers to the Cause Code within the Bearer Context when the response message (Create Bearer, Update Bearer, Delete Bearer*), indicates other than ACCEPTED or PARTIALLY_ACCEPTED. With this change, P-GW driver level populates the Bearer Context information from the Message level information for such scenarios. This information would further get passed to the SessMgr over the SNX interface. This helps re-use the Session Manager logic for handling the information within the Bearer Context without much change.

Allow Up to Three P-CSCF Addresses for IPv4 and IPv6 in P-GW

**Previous Behavior:**
1. CLI is used to configure the P-CSCF IPv4 and IPv6 addresses (primary and secondary) in APN.
2. CreateSessionReq is received requesting both P-CSCF IPv4 and IPv6 addresses.
3. CreateSessionResp is sent with 2 primary (1 IPv4 and 1 IPv6) and 2 secondary addresses (1 IPv6 and 1 IPv6).

**New Behavior:**
1. CLI has been enhanced to configure up to 3 IPv4 (priority 1-3) and 3 IPv6 (priority 1-3) P-CSCF addresses in APN.
2. CreateSessionReq is received requesting both P-CSCF IPv4 and IPv6 addresses.
3. CreateSessionResp is sent with 3 IPv4 and 3 IPv6 addresses.

Change for UDP Packet with Source Port 4500

**Previous Behavior:** P-GW handles UDP packet with source port 4500, destination port 434 as combo-phone request, triggering IPsec tunnel setup.

**New Behavior:** P-GW will not detect combo-phone request and treat UDP packet with source port4500, destination port 434 as normal MIP RRQ.

Configurable Subscriber State Management Audit Process

A new audit command and keywords in Context Configuration mode allow an operator to specify the start time and periodicity for generating Interchassis Session Recovery (ICSR) Service Redundancy Protocol (SRP) audit statistics. This audit ensures that two ICSR peers are in synch and identifies any discrepancies prior to scheduled or unscheduled switchover events.

Customer 4G Network Upgrade 3GPP Standard Baseline Release Compliance for P-GW / HSGW / ePDG

All PGW/HSGW/ePDG interfaces upgraded to support, at a minimum, inbound 3GPP R11 IEs that are needed to support features requested by customer.

- Network elements need to gracefully handle any new IE sent by Peer that is not supported by the network element.
- Network elements should comply to Interface specifications updated with the call flows and IEs necessary for the features.
- IE will be used as defined by 3GPP specifications and other relevant Diameter specifications.

The following interfaces are supported:

PGW: S6b, S5/S8, Gx, Gy, Rf, S2a, S2b, X3
HSGW: STa, S2a, Rf  
ePDG: SWn, SWm, S2b

**Default Behavior of UDP Checksum Optimization**

**Previous Behavior:** By default, UDP checksum was enabled, but no optimization attempted.

**New Behavior:** By default, attempt optimization of UDP checksum in UDP header of GTP-U packet using inner payload transport checksum.

**DNS Support for IPv4/IPv6 PDP Contexts**

**Previous Behavior:** P-GW was supporting DNS for IPv4 PDP context only.

**New Behavior:** This feature adds functionality in P-GW for PDN type IPv4v6. Previously, if an MS requested an IPv4 DNS address, P-GW did not send the IPv4 DNS address.

MS may request for DNS server IPv4 or IPv6 addresses using the Protocol Configurations Options IE (as a container or as part of IPCP protocol configuration request) in PDP Context Activation procedure for PDP Type IPv4, IPv6, or IPv4v6. In that case, the P-GW may return the IP address of one or more DNS servers in the PCO IE in the PDP Context Activation Response message. The DNS address(es) shall be coded in the PCO as specified in 3GPP TS 24.008.

For PDP Type IPv4v6, if MS requested DNS server IPv4 address, it did not return an IPv4 address. Support is now added to respond with address requested by MS.

AAA server may also provide DNS Server IP Address in Access-Accept Auth Response. In such cases, AAA provided DNS server IPs takes priority over the one configured under APN.

When DNS server address is requested in PCO configuration, the following preference would be followed:

1. DNS values received from RADIUS Server.
2. DNS values locally configured with APN.
3. DNS values configured at context level with `ip name-servers` CLI.

**DSCP Marking - GTP-U on per APN Basis**

This feature provides the flexibility to have a different DSCP marking table on per APN basis so that traffic on each of the APNs can be marked differently, depending on the needs of the APN.

The P-GW supports configurable DSCP marking of the outer header of a GTP-U tunnel packet based on a QCI/THP table for the S5/S8 and Gn/Gp interfaces. This feature allows configuring DSCP marking table on a per APN basis.

Previously, DSCP marking table was configured on P-GW service level. As part of this requirement, new CLI has been added to associate the qos-qci-mapping table in APN.

In order to be backward compatible with old configuration, if a DSCP marking table is associated with P-GW service and not with the APN, then the one in P-GW service will be used. If table is associated in both P-GW service and APN, then the one on APN will take precedence.

**Enhanced Granularity for Enabling S6b with a P-GW Service**

CLI command `authorize-with-hss` has been enhanced for greater P-GW S6b interface authorization control.

**GnGp Issue Resolved for GTP Echo Configuration Per Interface**

SM informs eGTP-C stack if the peer node is part of same PLMN (home) or different PLMN (roamer/visitor) based on MNC/MCC to avoid running APN-OI matching algorithm again.
Previous Behavior: Issue observed when performing GnGp Handoff when:
1. Moving from peer map non-associated GSN node to associated P-GW node.
2. The correct peer profile is not getting selected upon receiving MBR at P-GW.
As part of Modify Bearer Request processing, if the RAT type changed, the changes were getting updated later in clp (IP address change, MCC, MNC change) from the PDU, but the API was getting called earlier.
New Behavior: Call the peer profile fetch API as the last step in the MBR indication handling.

Gp Interface Support on P-GW

Previous Behavior: No AAR sent on S6b interface with new RAT-type at the time of Gn/Gp handoff.
New Behavior: AAR is sent towards S6b interface at the time of Gn/Gp handoff.

GTP Data Path Performance Improvements

GTP data path performance improvements implemented for P-GW.

IMS PDN Deactivation, UE is IDLE-APN Based Cause Code for PDN Deletion

New pdn-behavior CLI command in APN configuration has been added to control specific PDN behavior.

Previous Behavior: Currently, if the IMS PDN is not the last PDN being disconnected and UE is in Idle mode, MME
does not page the UE to indicate PDN is being disconnected. The network and UE are out of sync on the PDN
availability and no network-initiated procedures can be initiated. This causes a problem for IMS PDN as voice and other
services, such as SMS, cannot be delivered until UE reconnects to the IMS PDN; this will not happen until UE performs
the next service request, which could impact IMS services provided by the operator.

New Behavior: For P-GW or other network-initiated deletion (PCRF or AAA initiated, P-GW now includes the cause
“Reactivation requested” so MME pages the UE.

Important: Cause code should remain “Reactivation disallowed to APN” for Self Activation users.

Inter-RAT PS Handover Support for LTE Outbound Roamers on P-GW via Gp

Confirmed that P-GW supports Modify Bearer request from S-GW on S8 interface for 3G to 4G handover scenario.
Confirmed that P-GW supportsUpdate PDP Context Request from SGSN on Gp interface for 4G to 3G handover
scenario.

Local Switching of Framed Route Packets

When network-behind-mobile processing was enabled for a context configured on the Cisco ASR 5000 platform, any
default route available for that context was no longer used in forwarding egress traffic for that context. Network-behind-
mobile processing is enabled when Framed-Route attributes are present in the RADIUS Access-Accept messages for
subscribers. Even a single such call will turn on this processing, which will remain enabled until chassis reload.

Previous Behavior: MR-to-MR packets were sent out earlier from ASR 5000 in egress context and used to loopback to
ASR 5000 from external node.CSCzn28907 (Framed-route: Framed routes are not getting installed properly in the
forwarding table, though these attributes are supplied from AAA.) addressed this to do local switching, but it caused
side effect that default route was no longer used in context if present.
**New Behavior:** New functionality has been added to do local switching for MR-to-MR packets without sending packets out of ASR 5000. If packet is not MR-to-MR, then it will be forwarded and outbound packet will also match default route.

**NEMO Support in GGSN**

This feature now supports standards-based NEMO feature on GGSN, which allows operators to support Enterprise VPN service with the advantage of faster deployment and flexible bandwidth arrangement for customers.

**Previous Behavior:** NEMO support in P-GW was added in earlier StarOS releases.

**New Behavior:** In StarOS Release 15.0, support is added for GGSN as well so that NEMO can be supported for subscribers roaming out on 3G (UMTS/GERAN) networks.

---

**Important:** Use of Dynamic Network Mobile Routing (NEMO) for GGSN requires that a valid license key be installed. Contact your Cisco account representative for information on how to obtain a license.

NEMO (NEtwork MObility) provides wireless connectivity between enterprise core network and remote sites over 3G/4G network. The wireless connection can be used as either primary link or backup link. All the hosts in the remote site can directly communicate with hosts in the core network without using NAT.

Enterprise VPN service is one of the main use case for this feature. Fast deployment and flexible bandwidth arrangement for customers are some of the advantages of this service. Customers include banks, financial institutions, multi-sited enterprises, city public safety departments, transportation fleet, etc.

**New Bulkstats Addition in eGTP-C Per Message**

Statistics added to better track performance of GTPv2-C peers in the P-GW. Bulkstats added for reject causes in CSRsp, DSRsp, CBRsp, UBRsp, and DBRsp.

**P-GW - S2a PMIPv6 - 3GPP VSA Support for PBA Reject Status**

Confirmed that when the reject status is sent for a PBU via a PBA message, the Vendor Specific Mobility option is not set.

**P-GW - S2a PMIPv6 - Heartbeat Message Support**

P-GW now responds to heartbeat message requests from HSGW.

**P-GW - S2a PMIPv6 - Interworking with non-Cisco HSGW**

Confirmed that the P-GW will ignore the vendor-specific IEs, if any, and shall establish the calls.

**P-GW - S5 GTP - Interworking with non-Cisco S-GW**

Confirmed that the P-GW will ignore the vendor-specific IEs, if any, and shall establish the calls.

**P-GW Should Honor the TTL Provided by DNS for P-CSCF Resolution**

P-GW receives the P-CSCF FQDN from the AAA and resolves the FQDN via DNS to provide the IP addresses to the UE.

**Previous Behavior:** If the received TTL is less than 60 seconds, it was set to 60 internally.
New Behavior: If the received TTL is less than 60 seconds and honor-low-ttl is configured, it is now set to the configured honor-low-ttl value instead of 60.

After processing configured number of FQDNs, remaining would be set to previous default of 60 seconds

P-GW Support for Correction EPDN Sess for UICCless UE

Previous Behavior: Currently, the code assumes that the IMSI information is Mandatory for Trace Activation Support. Thus, when the UICCless UE is emergency attached or when the IMSI validation fails for the emergency attached UE, the following procedures are not supported:

- Indirect Data Forwarding using non-anchor S-GW
- Location Change Reporting (Impacts P-GW)
- Inter RAT, S1 based HO cancel
- Trace Activation (Impacts P-GW)

New Behavior: For the following messages:

- Create Indirect Data Forwarding Tunnel Request
- Change Notification Request/Response
- Relocation Cancel Request
- Trace Session Activation

The following changes are done:

- IMSI is marked as Conditional wherever it is currently Mandatory.
- IMEI IE is included conditionally for emergency attached UE which is UICCless.
- Indication IE is included to indicate if the IMSI is unauthenticated.

Changes are specific to Trace Session Activation extension to support both IMEI and IMSI instead of just IMSI.

P-GW Support for Suspend/Resume Notification and Inter-RAT HO for CS Fallback

Confirmed that P-GW supports Suspend/Resume Notification and Inter-RAT HO for CS Fallback.

PGW Support - S2a PMIPv6 Over IPv4 Transport

Customers will have new option to deploy and plan their network using new transport type.

Important: This feature is only supported for ASR 5500 platform.

Previous Behavior: S2a interface did not have transport support on IPv4.

New Behavior: This feature has introduced new transport-level support where PMIPv6 packet will be encoded with IPv6 and IPv4 headers. Packet will be sent on IPv4 transport.

Report Subscriber Summary per GTP-U Address

This feature helps in OAM to monitor the usage of a particular GTP-U address for different EPC bearers.

Previous Behavior: P-GW was not supporting the CLI to list the number of sessions per GTP-U local addresses in a gateway.
**New Behavior:** This feature enhanced the `show gtpu` CLI command to list the number of subscribers per GTP-U address in P-GW. The GTP-C control plane has a single IPv4 and/or IPv6 address. The GTP-U service can have multiple IPv4 and/or IPv6 addresses.

Following enhancements are done:

- `show gtpu` CLI enhanced to display the subscriber count per GTP-U address.
- `show gtpu statistics` CLI display is enhanced to display the usage of the IP addresses with subscriber counts.

**Send Default Bearer QoS and APN-AMBR Information in the Existing SM SGX Events**

- Code has been enhanced to send negotiated QoS to IMSA.
- SM provides the Default Bearer QoS and APN-AMBR info in the existing SM SGX events

**SM Changes for PCO Feature Phase 2 Support**

- Support for PCO updating using Gy interface.

**SM Support for Event Trigger charging-correlation-exchange**

- SM supports new event trigger for informing Charging Correlation Information.
  
  `CHARGING_CORRELATION_EXCHANGE (28)`

- The PCRF shall use this value in CCA and RAR commands to indicate that the PCEF shall report the access network charging identifier associated to one or more dynamic PCC Rules within the Access-Network-Charging-Identifier-Gx AVP. The Charging-Correlation-Indicator AVP with value `CHARGING_IDENTIFIER_REQUIRED` shall be provided.

- When used in a CCR command, this value indicates that an access network charging identifier has been assigned. The actual value shall be reported with the Access-Network-Charging-Identifier-Gx AVP.

**SM Support for Event Trigger tethering-flow-detection**

- SM now supports new event trigger for reporting tethered traffic.

**SM Support for GTP Echo Configuration Per Interface**

- This functionality is now supported. See [Node Functionality GTP Echo](#) for more information.

**SM Support for MINE Framework for Query Interface**

- **Previous Behavior:** Code was function pointer based.
- **New Behavior:** Redesigned to make it event driven where session information is passed via clp handle.

**SM Support for New S6b AVPs - Virtual-APN-Name**

- **Previous Behavior:** Virtual APN from S6b server is not handled.
- **New Behavior:** If virtual APN is received from S6b interface, then it is used as Gi-APN.

**SM Support for P-CSCF IPv6 Address Discovery**

- New flag added in for informing SGx about what UE has requested for P-CSCF address.
**Previous Behavior:** Currently, IMSA does the P-CSCF discovery whether or not UE has requested the P-CSCF address in the PCO of CPC/CSR.

**New Behavior:** IMSA now selects the P-CSCF address only if it is requested from the UE. SM forwards the request to IMSA so that IMSA can select the IPv6 P-CSCF address based on this request.

**SM Support for Preventing Usage Bucket Loss When PCRF is Unreachable**

This functionality is now supported.

Added SM support for this feature.

**SM Support for Sponsor Identity**

Confirmed support of newAVPs Sponsor-Identity and Application-Service-Provider-Identity.

**SM Support for SP WiFi - P-GW Coupled Web Authentication**

Enhanced P-GW capability to support web authentication via Gx interface. Capability includes:

- Enhanced Gx definition to support the signalling of an authentic user ID (NAI or MSISDN) over the Gx/RAR.
- The ability to account separately for usage prior to successful web and post web authentication.
- The ability to include the authenticated user identity in charging records.

**SP WiFi - P-GW MAG Scalability**

Confirmed that P-GW supports one million MAGs.

**SRVCC PS-to-CS Handover Indication Support**

This feature helps in notifying the PCRF about the exact reason for PCC rule deactivation on Voice bearer deletion. This exact cause will help PCRF to then take further action appropriately.

**Previous Behavior:**

1. Support of voice bearer flag in BearerFlags IE was not present in Delete Bearer Cmd initiated by MME.
2. Support of new Rule Failure Code PS_TO_CS_HANDOVER in Charging Rule Report was not present.

**New Behavior:** This feature ensures complete compliance for SRVCC, including support for PS-to-CS handover indication when voice bearers are released. The support for SRVCC feature was first added in StarOS Release 12.2.

SRVCC service for LTE comes into the picture when a single radio User Equipment (UE) accessing IMS-anchored voice call services switches from the LTE network to the Circuit Switched domain while it is able to transmit or receive on only one of these access networks at a given time. This removes the need for a UE to have multiple Radio Access Technology (RAT) capability.

1. After handing over the PS sessions to the target, the source MME shall remove the voice bearers by deactivating the voice bearer(s) towards S-GW/P-GW and setting the VB (Voice Bearer) flag of Bearer Flags IE in the Delete Bearer Command message (TS 29.274 v9.5.0).
2. If the IP-CAN bearer termination is caused by the PS to CS handover, the PCEF may report related PCC rules for this IP-CAN bearer by including the Rule-Failure-Code AVP set to the value PS_TO_CS_HANDOVER (TS 29.212 v10.2.0 and TS 23.203 v10.3.0).

Support for new AVP PS-to-CS-Session-Continuity (added in 3GPP Release 11) inside Charging Rule Install, which indicates if the bearer is selected for PS to CS continuity is not added.

**Support “show subs full peer-address <>” for eHRPD calls in P-GW**
Support added to `show subscribers` CLI command to find sessions in P-GW specific to MAG address, and also to `clear subscribers` to clear sessions specific to a MAG address.

**P-GW Command Changes as of September 30, 2013**

This section provides information on P-GW command changes in release 15.0.

**Important:** For more information regarding commands in this section, refer to the *Command Line Interface Reference* for this release.

**New P-GW Commands**

This section identifies new P-GW commands available in release 15.0.

**description**

The following new command configures a short description for the specified peer profile.

```plaintext
configure

    peer-profile service-type pgw-access { default | name profile_name } [ -noconfirm ]
        description description
        no description
    end
```

**gtpc**

The following new command configures the GTP-C settings for the specified peer profile.

```plaintext
configure

    peer-profile service-type pgw-access { default | name profile_name } [ -noconfirm ]
        gtpc { echo { interval seconds | retransmission-timeout seconds } | max-retransmissions number | retransmission-timeout seconds }
        default gtpc { echo [ interval | retransmission-timeout ] | max-retransmissions | retransmission-timeout }
        no gtpc echo
    end
```

Notes:

- `gtpc echo interval seconds` must be an integer from 60 to 3600. Default: 60
- `gtpc echo retransmission-timeout seconds` must be an integer from 1 to 20. Default: 5
• **gtpc max-retransmissions** `number` must be an integer from 0 to 15.
  Default: 4
• **gtpc retransmission-timeout** `seconds` must be an integer from 1 to 20.
  Default: 5

**heartbeat**

The following command configures the PMIPv6 heartbeat message interval, retransmission timeout, and max retransmission for the LMA Service.

```bash
configure
  context context_name
    lma-service lma_name
      heartbeat { interval seconds | retransmission { max number | timeout seconds } }
      default heartbeat { interval | retransmission { max | timeout } }
    no heartbeat
  end
```

Notes:
• **interval**: The interval in seconds at which heartbeat messages are sent.
  `seconds` must be an integer from 30 to 2600. Default: 60
• **retransmission max**: The maximum number of heartbeat retransmissions allowed.
  `number` must be an integer from 0 to 15.
  Default: 3
• **retransmission timeout**: The timeout in seconds for heartbeat retransmissions.
  `seconds` must be an integer from 1 to 20.
  Default: 3

**ip guarantee**

This command enables and disables local switching of framed route packets.

```bash
config
  context <context_name>
    [ no ] ip guarantee framed-route local-switching
  end
```

Notes:
• By default, this CLI will be enabled.
• This functionality will be applicable only when there are some NEMO/framed route sessions in a context.
**mobile-ip min-reg-lifetime-override**

This command specifies the minimum registration timer to override the platform-wide default on an enterprise basis. With this command, NEMO traffic could be re-routed symmetrically to an alternate carrier within the specified number of seconds following a failure on the primary communication path.

```plaintext
configure
  context context_name
    apn apn_name
      mobile-ip min-reg-lifetime-override { seconds | infinite }
      { default | no } mobile-ip min-reg-lifetime-override
    end
```

Notes:
- **seconds**: specifies the minimum registration interval in seconds as an integer from 1 to 65534. Default: 600
- **infinite**: Sets the minimum registration interval as “infinite” (forever) for this subscriber.
- **no**: Deletes the registration interval entered via this command.

**pdn-behavior**

This command configures specific PDN behavior.

```plaintext
configure
  context context_name
    apn apn_name
      pdn-behavior { custom1 | ims }
      { default | no } pdn-behavior
    end
```

Notes:
- **custom1**: Configures APN as a Custom1 (well-known) APN. Re-auth Requested reason code returned for PDN disconnect.
- **ims**: Configures APN as an IMS APN. Re-auth Requested reason code returned for PDN disconnect.
- **default | no**: Configures APN as “Normal”.

**peer-map**

The following new command creates a peer map and enters the Peer Map Configuration mode. This new command mode enables the operator to map and LTE Policy to a peer profile based on matching criteria and precedence for the criteria.

```plaintext
configure
```
### lte-policy

```plaintext
peer-map map_name [ -noconfirm ]

no peer-map map_name

end
```

### peer-profile

The following command creates a P-GW peer profile and enters the Peer Profile Configuration mode.

```plaintext
configure

peer-profile service-type pgw-access { default | name profile_name } [ -noconfirm ]

no peer-profile service-type pgw-access name profile_name

end
```

Note:
- A maximum of 64 peer profiles can be configured.

### precedence

The following new command configures the matching criteria and precedence for mapping an LTE Policy with a peer profile.

```plaintext
configure

lte-policy

peer-map map_name [ -noconfirm ]

precedence priority match-criteria { all peer-profile-name profile_name | peer-ip-address { ip_address | ip_address/mask } | serving-plmnid mcc mcc mcc mcc | peer-profile-name profile_name | serving-plmnid mcc mcc mcc mcc | peer-ip-address { ip_address | ip_address/mask } | peer-profile-name profile_name }

no precedence priority

end
```

Notes:
- Precedence 1 has highest priority.
  - `priority` must be an integer from 1 to 1024.
- A maximum of 1024 precedence entries can be configured.
- To map a peer to a profile when there is no specific criteria required, use the `all` keyword.
- `mcc` must be a three-digit number between 100 and 999.
- `mnc` must be a two- or three-digit number between 00 and 999.
session trace random

The following new command has been added to the Exec Mode to enable or disable the subscriber session trace functionality based on a the random trace on the network element. If enabled, the subscriber selection will be based on random logic on all instance of session on a specified UMTS/EPS network element. It also clears/resets the statistics collected for subscriber session trace on a system.

```
[ no ] session trace random random_num network-element { ggsn | pgw } [ interface { all | interface } ] [ collection-entity ip_address ]
```

session trace signaling

The following new command has been added to the Exec Mode to enable or disable the subscriber session trace functionality based on signaling information on one or all instance of session on a specified UMTS/EPS network element. It also clears/resets the statistics collected for subscriber session trace on a system.

```
[ no ] session trace signaling network-element { ggsn | pgw }
```

show peer-profile

The following new command displays configuration of the specified peer profile.

```
show peer-profile { all | full { all | name profile_name } | name profile_name }
```

Modified P-GW Commands

This section identifies P-GW commands modified in release 15.0.

associate

The new keyword peer-map associates an LTE Policy peer map with a P-GW service.

```
configure

  context context_name

  pgw-service svc_name

    associate peer-map map_name

    no associate peer-map

  end
```

associate

The new keyword qci-qos-mapping has been added to configure DSCP marking of the outer header of a GTP-U tunnel packet based on a QCI table. DSCP marking shall be supported on a per APN basis.

```
configure

  context context_name

  apn apn_name
```
qci-qos-mapping table_name
no qci-qos-mapping
end

authorize-with-hss

This command enables or disables subscriber session authorization via a Home Subscriber Server (HSS) over an S6b Diameter interface. This feature is required to support the interworking of GGSN with P-GW and HA. New keywords have been added to enhance granularity for enabling S6b with a P-GW service.

configure

context context_name

pgw-service service_name

authorize-with-hss [ egtp | lma ] [ report-ipv6-addr ]

{ default | no } authorize-with-hss
end

Notes:
• egtp enables S6b authorization for EGTP only.
• lma enables S6b authorization for LMA only.

clear subscribers

The pgw-address keyword now can be used to filter for all running services. Previously this keyword was applicable only for S-GW and SAEGW services. Only those sessions which match the specified filters will be cleared.

clear subscribers pgw-address ipv4/ipv6_address [ filter_keywords ] [ verbose ] [ -noconfirm ]

clear subscribers hsgw-only

The hsgw-only keyword has been added to this command. This CLI command will filter all the sessions emerging from HSGW. The results can be filtered further based on other options selected. Only those sessions which match the specified filters will be cleared.

clear subscribers hsgw-only [ filter_keywords ] [ verbose ] [ -noconfirm ]

clear subscribers pgw-only

The mag-address keyword has been added to this command. This CLI command will first filter all the sessions emerging from P-GW and then further filter the ones that go to the specified MAG address. The results can be filtered further based on other options selected. Only those sessions which match the specified filters will be cleared.

clear subscribers pgw-only mag-address ipv4/ipv6_address [ filter_keywords ] [ verbose ] [ -noconfirm ]
egtp overcharge-protection

**Corrected Content:** This section includes corrections to previously published content. The previous content stated that, “Overcharging Protection functionality has been implemented as lab quality”, which is incorrect. Overcharging Protection functionality has been implemented as deploy quality.

Configures handling of eGTP related procedures.

The new keyword `overcharge-protection` has been added to control overcharging protection functionality on a P-GW service. By default, overcharging protection will not be enabled.

```plaintext
configure
  context context_name
  pgw-service service_name
    [ default | no ] egtpc overcharge-protection
  end
```

Notes:
- `overcharge-protection` configures overcharging protection by temporarily not charging during loss of radio coverage.

egtp sgw-restoration

Configures handling of eGTP related procedures.

The new keyword `sgw-restoration` has been added to enable S-GW restoration functionality and configure session hold timeout on a P-GW service. By default, S-GW restoration will not be enabled.

```plaintext
configure
  context context_name
  pgw-service service_name
    egtpc sgw-restoration session-hold timeout seconds
    { default | no } egtpc sgw-restoration session-hold
  end
```

Notes:
- `session-hold timeout` configures session hold timer for S-GW restoration.
- `seconds` must be an integer from 1 to 3600. Default: 0 (disabled).
- On S-GW failure indication, P-GW shall check if S-GW restoration feature is enabled or not. If enabled, P-GW shall maintain all the affected sessions for session-hold timeout. After session-hold timeout, P-GW shall clear all the sessions which are not recovered yet.

pco-options

The new keyword `link-mtu` has been added to configure APN to include link MTU in PCO IE.
configure

    context context_name

    apn apn_name

    pco-options { custom1 [ ue-requested ] | link-mtu bytes }
    { default | no } pco-options [ custom1 | link-mtu ]

end

Notes:
- link-mtu configures APN to include link MTU in PCO IE, if it is requested by UE.
- bytes must be an integer from 1280 to 2000. Default: 1500

p-cscf

Enables use of locally configured Proxy Call Session Control Function (P-CSCF) addresses or a Fully Qualified Domain Name (FQDN).

The new keyword priority has been added to specify the priority for P-CSCF address for the APN.

configure

    context context_name

    apn apn_name

    p-cscf { fqdn fqdn | priority address_ priority [ ip IPv4_address | ipv6 IPv6_address ] }

    no p-cscf { fqdn fqdn | priority address_ priority [ ip | ipv6 ] }

end

Notes:
- address_ priority is an integer from 1 to 3. 1 is the highest priority.

qci

The new keyword mpls-exp-value has been added to allow QCI-to-MPLS EXP mappings

configure

    qci-qos-mapping table_name


end
show gtpu

Displays the number of GTP-U sessions per local address for a given GTP-U service.
The new keyword `local-addresses` has been added to display the number of GTPV0 and GTPV1 sessions per local address per active service.

`show gtpu local-addresses`

show gtpu statistics

Displays GPRS Tunneling Protocol user plane (GTP-U) statistics and counters.
The new keyword `local-address` has been added to display the session information per GTP-U address.

`show gtpu statistics peer-address ipv4/ipv6_address`

Note:

- This command will display the same fields as displayed for `peer-address`.

show lte-policy peer-map

The new keyword `peer-map` displays configuration of the specified LTE Policy peer map.

`show lte-policy peer-map { name map_name | summary }`

show subscribers

The `pgw-address` keyword now can be used to filter for all running services. Previously this keyword was applicable only for S-GW and SAEGW services.

`show subscribers pgw-address ipv4/ipv6_address [ filter_keywords ] [ | { grep grep_options | more } ]`

show subscribers pgw-only

The `mag-address` keyword has been added to this command. This CLI command will first filter all the sessions emerging from P-GW and then further filter the ones that go to the specified MAG address. The results can be filtered further based on other options selected.

`show subscribers pgw-only mag-address ipv4/ipv6_address [ filter_keywords ] [ | { grep grep_options | more } ]`

show subscribers hsgw-only

The `pgw-address` keyword has been added to this command. This CLI command will first filter all the sessions emerging from HSGW and then further filter the ones that go to the specified P-GW address. The results can be filtered further based on other options selected.

`show subscribers hsgw-only pgw-address ipv4/ipv6_address [ filter_keywords ] [ | { grep grep_options | more } ]`

udp-checksum
This command now allows no optimization attempt over UDP checksum in UDP header of GTP-U packet.

```
configure
c

context context_name
gtpu-service service_name

udp-checksum { no-optimize | optimize }
{ default | no } udp-checksum

end
```

**Deprecated P-GW Commands**

This section identifies deprecated P-GW commands that are no longer supported in release 15.0.

None for this release.

**P-GW Performance Indicator Changes as of September 30, 2013**

This section provides information on P-GW performance indicator changes in release 15.0.

---

**Important:** For more information regarding bulk statistics and output fields and counters in this section, refer to the *Statistics and Counters Reference* for this release.

---

**New P-GW Bulk Statistics**

This section identifies new P-GW bulk statistics available in release 15.0.

**New in the eGTP-C Schema**

The following bulkstats have been added:

- tun-rev-cresessNorsp
- tun-rev-cresessDiscard

The following bulkstats have been added for Create Session Response:

- tun-sent-cresessrespdeniedCtxtNotFound
- tun-sent-cresessrespdeniedInvalidMsgFormat
- tun-sent-cresessrespdeniedInvalidLength
- tun-sent-cresessrespdeniedMandIEIncorrect
- tun-sent-cresessrespdeniedMandIEMissing
- tun-sent-cresessrespdeniedNoResourcesAvl
- tun-sent-cresessrespdeniedMissingUnknownApn
- tun-sent-cresessrespdeniedPrefPdnTypeUnsupported
- `tun-sent-cresessrespdene...AllDynamicAddrOccupied`
- `tun-sent-cresessrespdene...ServiceDenied`
- `tun-sent-cresessrespdene...UserAuthFailed`
- `tun-sent-cresessrespdene...ApnAccessDenied`
- `tun-sent-cresessrespdene...RequestRejected`
- `tun-sent-cresessrespdene...CondIEMissing`
- `tun-sent-cresessrespdene...ApnRstTypeIncompatible`
- `tun-sent-cresessrespdene...ImsiNotKnown`
- `tun-sent-cresessrespdene...OtherCause`

The following `bulkstats` have been added:

- `tun-recv-crecessrespsDiscard`
- `tun-recv-crebearDiscard`
- `tun-recv-crebearNorsp`
- `tun-recv-crebearrespDiscard`

The following `bulkstats` have been added for Create Bearer Response:

- `tun-recv-crebearrespdene...CtxtNotFound`
- `tun-recv-crebearrespdene...SvcNotSupported`
- `tun-recv-crebearrespdene...InvalidMsgFormat`
- `tun-recv-crebearrespdene...MandIElIncorrect`
- `tun-recv-crebearrespdene...MandIEMissing`
- `tun-recv-crebearrespdene...CondIEMissing`
- `tun-recv-crebearrespdene...NoResourcesAvl`
- `tun-recv-crebearrespdene...SemanticErrinTFT`
- `tun-recv-crebearrespdene...SyntacticErrinTFT`
- `tun-recv-crebearrespdene...SemanticErrinPktFltr`
- `tun-recv-crebearrespdene...SyntacticErrinPktFltr`
- `tun-recv-crebearrespdene...UnableToPageUE`
- `tun-recv-crebearrespdene...UENotResponding`
- `tun-recv-crebearrespdene...UnableToPageUeSuspend`
- `tun-recv-crebearrespdene...UERefuses`
- `tun-recv-crebearrespdene...RequestRejected`
- `tun-recv-crebearrespdene...InvalidLenPiggybkMsg`
- `tun-recv-crebearrespdene...InvalidRemotePeerReply`
- `tun-recv-crebearrespdene...PeerNotResponding`
- `tun-re cv-cre bearres pdeniedTempRejDueToHOProgress`
- `tun-re cv-cre bearres pdeniedDeniedInRat`
- `tun-re cv-cre bearres pdeniedOtherCause`

The following bulkstats have been added:
- `tun-re cv-b earres cmdDiscard`
- `tun-re cv-b earres cmdNorsp`
- `tun-re cv-bear rescmd-failDiscard`
- `tun-re cv-modbearreqDiscard`
- `tun-re cv-modbearreqNorsp`
- `tun-re cv-modbearrespDiscard`
- `tun-re cv-delsessreqDiscard`
- `tun-re cv-delsessreqNorsp`

The following bulkstats have been added for Delete Session Response:
- `tun-s en-delsessrespdeniedCtxtNotFound`
- `tun-s en-delsessrespdeniedInvalidMsgFormat`
- `tun-s en-delsessrespdeniedMandIEIncorrect`
- `tun-s en-delsessrespdeniedMandIEMissing`
- `tun-s en-delsessrespdeniedNoResourcesAvl`
- `tun-s en-delsessrespdeniedOtherCause`

The following bulkstats have been added:
- `tun-re cv-delsessrespDiscard`
- `tun-re cv-del bearreqDiscard`
- `tun-re cv-del bearreqNorsp`
- `tun-re cv-del bearrespDiscard`

The following bulkstats have been added for Delete Bearer Response:
- `tun-re cv-del bearrespdeniedCtxtNotFound`
- `tun-re cv-del bearrespdeniedInvalidMsgFormat`
- `tun-re cv-del bearrespdeniedMandIEIncorrect`
- `tun-re cv-del bearrespdeniedMandIEMissing`
- `tun-re cv-del bearrespdeniedCondIEMissing`
- `tun-re cv-del bearrespdeniedNoResourcesAvl`
- `tun-re cv-del bearrespdeniedRequestRejected`
- `tun-re cv-del bearrespdeniedUnableToPageUeSuspend`
- `tun-re cv-del bearrespdeniedInvalidRemotePeerReply`
- tun-recv-dlcbearerrespdeniedPeerNotResponding
- tun-recv-dlcbearerrespdeniedTempRejDueToHOProgress
- tun-recv-dlcbearerrespdeniedOther

The following bulkstats have been added:
- tun-recv-dlknottifDiscard
- tun-recv-dlknottifNorsp
- tun-recv-dlknottifackDiscard
- tun-recv-dlinkdatafailDiscard
- tun-recv-relaccbearreqDiscard
- tun-recv-relaccbearreqNorsp
- tun-recv-relaccbearrespDiscard
- tun-recv-modbearcmdDiscard
- tun-recv-modbearcmdNorsp
- tun-recv-modbearfailDiscard
- tun-recv-dlcbearcmdDiscard
- tun-recv-dlcbearcmdNorsp
- tun-recv-dlcbearfailDiscard
- tun-recv-updbearreqDiscard
- tun-recv-updbearreqNorsp
- tun-recv-updbearrespDiscard

The following bulkstats have been added for Update Bearer Response:
- tun-recv-updbearrespdeniedCtxtNotFound
- tun-recv-updbearrespdeniedInvalidMsgFormat
- tun-recv-updbearrespdeniedMandIEIncorrect
- tun-recv-updbearrespdeniedMandIEMissing
- tun-recv-updbearrespdeniedNoResourcesAvl
- tun-recv-updbearrespdeniedSemanticErrInTFT
- tun-recv-updbearrespdeniedSyntacticErrInTFT
- tun-recv-updbearrespdeniedSemanticErrInPktFltr
- tun-recv-updbearrespdeniedSyntacticErrInPktFltr
- tun-recv-updbearrespdeniedUENotResponding
- tun-recv-updbearrespdeniedUERefuses
- tun-recv-updbearrespdeniedUnableToPageUE
- tun-recv-updbearrespdeniedRequestRejected
- tun-recev-updbearrespdeniedUnableToPageUeSuspend
- tun-recev-updbearrespdeniedCondIEMissing
- tun-recev-updbearrespdeniedInvalidRemotePeerReply
- tun-recev-updbearrespdeniedPeerNotResponding
- tun-recev-updbearrespdeniedTempRejDueToHOProgress
- tun-recev-updbearrespdeniedOtherCause

The following bulkstats have been added:
- tun-recev-creinddatafwdngreqDiscard
- tun-recev-creinddatafwdngreqNorsp
- tun-recev-delinddatafwdngrspDiscard
- tun-recev-delinddatafwdngrqDiscard
- tun-recev-delinddatafwdngreqNorsp
- tun-recev-changenotfreqDiscard
- tun-recev-changenotfreqNorsp
- tun-recev-changenotfrespDiscard

The following bulkstats have been added for P-GW Restart Notification support:
- tun-sent-pgwRstnotfreq
- tun-sent-retranspgwRstnotfreq
- tun-sent-noRspPgwrstnotfreq
- tun-recev-pgwRstnotfackp
- tun-recev-pgwRstnotfackpaccept
- tun-recev-pgwRstnotfackpdenied
- tun-recev-discardPgwrstnotfack

The following bulkstats have been added:
- csfb-recev-suspendnotfDiscard
- csfb-recev-suspendnotfNorsp
- csfb-recev-suspendackDiscard
- csfb-recev-resumenotfDiscard
- csfb-recev-resumenotfNorsp
- csfb-recev-resumeackDiscard

The following bulkstats have been added to reflect throttling related statistics:
- tun-sent-crebear-throttle-succeed
- tun-sent-crebear-throttle-queued
• tun-sent-crebear-throttle-dropped
• tun-sent-retranscrebear-throttle-succeed
• tun-sent-retranscrebear-throttle-queued
• tun-sent-retranscrebear-throttle-dropped
• tun-sent-updbearreq-throttle-succeed
• tun-sent-updbearreq-throttle-queued
• tun-sent-updbearreq-throttle-dropped
• tun-sent-retransupdbearreq-throttle-succeed
• tun-sent-retransupdbearreq-throttle-queued
• tun-sent-retransupdbearreq-throttle-dropped
• tun-sent-delbearreq-throttle-succeed
• tun-sent-delbearreq-throttle-queued
• tun-sent-delbearreq-throttle-dropped
• tun-sent-retransdelbearreq-throttle-succeed
• tun-sent-retransdelbearreq-throttle-queued
• tun-sent-retransdelbearreq-throttle-dropped

The following bulkstats have been added to reflect incoming throttling:

• msgs-inc-rate-limited
• msgs-inc-rl-scheduled
• msgs-inc-rl-curr-queued
• msg-inc-rl-drop-queue
• msg-inc-rl-throttled

The following GTP path bulkstats have been added for Request Messages:

• total-sent-req
• total-sent-retransReq
• total-recv-req
• total-recv-retransReq
• total-recv-reqDiscarded
• total-recv-noRspReq

The following GTP path bulkstats have been added for Response Messages:

• total-sent-rsp
• total-sent-rspAccept
• total-sent-rspDenied
• total-sent-rspRetrans
- total-recv-resp
- total-recv-rspAccept
- total-recv-rspDenied
- total-recv-rspDiscarded

The following bulkstats have been added:

- mobility-recv-ctxreqDiscard
- mobility-recv-ctxreqNorsp
- mobility-recv-ctxrspDiscard
- mobility-recv-ctxrspNorsp
- mobility-recv-ctxackDiscard
- mobility-recv-idtreqDiscard
- mobility-recv-idtreqNorsp
- mobility-recv-idtrspDiscard
- mobility-recv-fwdrelreqDiscard
- mobility-recv-fwdrelreqNorsp
- mobility-recv-fwdrelrspDiscard
- mobility-recv-fwdacnnotfNorsp
- mobility-recv-fwdacnnotfDiscard
- mobility-recv-fwdaccackDiscard
- mobility-recv-fwdrelcmpnotfDiscard
- mobility-recv-fwdrelcmpnotfNorsp
- mobility-recv-fwdrelcmpackDiscard
- mobility-recv-relcancelreqDiscard
- mobility-recv-relcancelreqNorsp
- mobility-recv-relcancelrspDiscard
- mobility-recv-alertmmenotfDiscard
- mobility-recv-alertmmenotfNosp
- mobility-recv-alertmmeackDiscard
- mobility-recv-ueactivitynotfDiscard
- mobility-recv-ueactivitynotfNorsp
- mobility-recv-ueactivityackDiscard
- mobility-recv-detchnotfDiscard
- mobility-recv-detchnotfNorsp
- mobility-recv-detchackDiscard
- srvcc-recv-pstocsrspDiscard
- srvcc-recv-pstoscempnotfDiscard
- srvcc-recv-pstoscancelackDiscard

**New in the LMA Schema**

The following bulkstats have been added for PMIPv6 heartbeat statistics:
- lma-txhbreqinitial
- lma-txhbreqretrans
- lma-txhbrsptotal
- lma-rxhbreqtotal
- lma-rxhbrsptotal
- lma-rxhbrspbinderror
- lma-rxhbdiscardtotal
- lma-rxhbdiscarderror
- lma-rxhbinvalidbufflen
- lma-rxhbrspunknownpeer
- lma-rxhbrsseqnummismatch
- lma-rxhbrsprstctrmismatch
- lma-pathfailurestotal
- lma-pathfailrstctrchange
- lma-pathfailnohbrsprcvd

**New in the P-GW Schema**

The following bulkstats have been added for S-GW restoration:
- sessstat-sgwrstr-instrstate
- sessstat-sgwrstr-recovered
- sessstat-sgwrstr-released
- sessstat-sgwrstr-uplktkd
- sessstat-sgwrstr-uplktkd
- sessstat-sgwrstr-dnlktkd
- sessstat-sgwrstr-dnlktkd

**Corrected Content:** This section includes corrections to previously published content. The previous content stated that, “Overcharging Protection functionality has been implemented as lab quality”, which is incorrect. Overcharging Protection functionality has been implemented as deploy quality.

The following bulkstats have been added for overcharging protection:
- sessstat-ovrchrgprtctn-uplktkd
• sessstat-ovrchrgprtctn-uplkbtyedrop
• sessstat-ovrchrgprtctn-dnlkpktdrop
• sessstat-ovrchrgprtctn-dnlkbtyedrop

**Modified P-GW Bulk Statistics**

This section identifies P-GW bulk statistics modified in release 15.0.
None for this release.

**Deprecated P-GW Bulk Statistics**

This section identifies deprecated P-GW bulk statistics that are no longer supported in release 15.0.
None for this release.

**New P-GW Output Fields and Counters**

This section identifies new P-GW show command output fields and counters available in release 15.0.

**show apn name**

The following fields have been added to show PCO values assigned to custom1 and link MTU:
• PCO Options
  • custom1 Mode
  • link MTU
The following field has been added to show the configuration of the mobile-ip min-reg-lifetime timer:
• mobile-ip min-reg-lifetime

**show apn statistics all**

**Corrected Content:** This section includes corrections to previously published content. The previous content stated that, “Overcharging Protection functionality has been implemented as lab quality”, which is incorrect. Overcharging Protection functionality has been implemented as deploy quality.

The following counters have been added to display overcharging protection stats for this APN:
• UL Ovrchrg Prtctn byte drop
• UL Ovrchrg Prtctn pkt drop
• DL Ovrchrg Prtctn byte drop
• DL Ovrchrg Prtctn pkt drop

**show egtpc peers**

The following field has been added to display the Node Features capability of the peer, for the Node functionality GTP Echo feature:
• Node Feature
**show egtp-service all**

The following field has been added to display the node features enabled in each egtpc service, such as P-GW Restart Notification, for the Node functionality GTP Echo feature:

- GTPC Node Feature

**show egtpc statistics**

The following fields and counters have been added to display outgoing GTP throttling stats information:

- Create Bearer Request (RLF)/Update Bearer Request (RLF)/Delete Bearer Request (RLF)
  - Total TX/Initial TX/Retrans TX
  - Succeed
  - Queued
  - Dropped

The following counters have been added to display incoming GTP throttling stats information:

- EGTPC Incoming Throttling
- Total Messages Rate Limited
- Total Messages Scheduled
- Total Messages Currently Queued
- Total Messages Dropped From Queue
- Total Messages Throttled

**show gtpu-service all**

The following new field has been added to this command to display whether UDP checksum optimization in UDP header. is enabled or disabled:

- GTPU UDP Checksum

**show gtpu statistics peer-address**

The following new counters have been added to this command to display the number of “Supported Extension Header” messages sent and received by the gateway:

- SuppExtnHdr Tx
- SuppExtnHdr Rx

**show lma-service all**

The following fields have been added to show the configuration of the heartbeat command:

- Heartbeat Support
- Heartbeat Interval
- Heartbeat Retransmission timeout
- Heartbeat Max Retransmissions
show lma-service statistics

The following counters have been added to show heartbeat statistics:

- Heartbeat Request
  - Total TX
  - Total RX
  - Initial TX
  - Initial RX
  - Retrans TX
- Heartbeat Response
  - Total TX
  - Total RX
  - Bind Error
- Heartbeat Messages Discarded
  - Total
  - Decode error
  - Invalid Buffer Length
  - Heartbeat Rsp From Unknown Peer
  - Heartbeat Rsp Seq. Num Mismatch
  - Heartbeat Rsp Restart Ctr Opt missing
  - Reasons for path failure
  - Restart counter change
  - No Heartbeat Response received
  - Total path failures detected

show lte-policy peer-map name

The following fields display configuration information of the precedence entries within the specified LTE Policy peer map:

- Peer Map <name>
- precedence <n>

show peer-profile full all

The following fields display configuration information for all peer profiles:

- <service-type> Peer Profiles
- Peer Profile Name
- Description
- GTPC echo
- GTPC echo retransmission timeout
- GTPC echo interval
- GTPC max retransmissions
- GTPC retransmission timeout
- Lawful-intercept

**show pgw-service all**

**Corrected Content:** This section includes corrections to previously published content. The previous content stated that, "Overcharging Protection functionality has been implemented as lab quality", which is incorrect. Overcharging Protection functionality has been implemented as deploy quality.

The following fields have been added to display configuration information for S-GW restoration on this P-GW service:

- EGTP SGW Restoration Handling
  - Session Hold Timer
  - Timeout

The following field has been added to display configuration information for overcharging protection on this P-GW service:

- EGTP Overcharge Protection

**show pgw-service statistics all**

**Corrected Content:** This section includes corrections to previously published content. The previous content stated that, "Overcharging Protection functionality has been implemented as lab quality", which is incorrect. Overcharging Protection functionality has been implemented as deploy quality.

The following counters have been added to display S-GW restoration for this P-GW node:

- SGW Restoration Statistics
  - PDNs Total
    - In Restoration State
    - Recovered
    - Released
  - Drops During SGW Restoration State
    - Packets
    - Bytes

The following counters have been added to display overcharging protection for this P-GW node:

- Drops Due To Overcharge Protection
  - Packets
  - Bytes

**show session disconnect-reasons verbose**

The following new disconnect reason was added in support of SRVCC PS-to-CS handover indication:

- srvcc-ps-to-cs-handover(538)
show session trace subscriber

The following field has been added to display subscriber session trace functionality type:

- Trace Type

show subscribers full

**Corrected Content:** This section includes corrections to previously published content. The previous content stated that, “Overcharging Protection functionality has been implemented as lab quality”, which is incorrect. Overcharging Protection functionality has been implemented as deploy quality.

The following counters have been added to display overcharging protection for all subscribers:

- in packet dropped overcharge protection
- in bytes dropped overcharge protection
- out packet dropped overcharge protection
- out bytes dropped overcharge protection

**Important:** When a session is in overcharge protection state, not all the downlink packets will be dropped; however, downlink packets will be rate limited. Current configuration allows one downlink packet per minute towards S-GW without charging it, if any downlink packets come to P-GW. P-GW will not generate any packets of its own.; separate debug stats have been added for P-GW.

show subscribers pgw-only full all

The following field has been added to display the peer profile for this subscriber:

- Network Peer Profile

The following field and counters have been added to display S-GW restoration:

- Bearer State
  - in packet dropped sgw restoration state
  - in bytes dropped sgw restoration state
  - out packet dropped sgw restoration state
  - out bytes dropped sgw restoration state

**Corrected Content:** This section includes corrections to previously published content. The previous content stated that, “Overcharging Protection functionality has been implemented as lab quality”, which is incorrect. Overcharging Protection functionality has been implemented as deploy quality.

The following field and counters have been added to display overcharging protection:

- Bearer State
  - in packet dropped overcharge protection
  - in bytes dropped overcharge protection
  - out packet dropped overcharge protection
  - out bytes dropped overcharge protection

The following fields and counters have been added to display PCRF authorized QoS:
• PCRF Authorized Bearer QoS
  • QCI
    • ARP
      • PCI
      • PL
      • PVI
    • MBR Uplink(bps)
    • MBR Downlink(bps)
    • GBR Uplink(bps)
    • GBR Downlink(bps)
    • APN AMBR uplink
    • APN AMBR downlink

**Important:** This functionality has been implemented as lab quality.

**show subscribers summary**

**Corrected Content:** This section includes corrections to previously published content. The previous content stated that, “Overcharging Protection functionality has been implemented as lab quality”, which is incorrect. Overcharging Protection functionality has been implemented as deploy quality.

The following counters have been added to display overcharging protection for all subscribers:

• in bytes dropped ovrchrgPtn
• in packet dropped ovrchrgPtn
• out bytes dropped ovrchrgPtn
• out packet dropped ovrchrgPtn

**Important:** When a session is in overcharge protection state, not all the downlink packets will be dropped; however, downlink packets will be rate limited. Current configuration allows one downlink packet per minute towards S-GW without charging it, if any downlink packets come to P-GW. P-GW will not generate any packets of its own; separate debug stats have been added for P-GW.

**Modified P-GW Output Fields and Counters**

This section identifies modified P-GW show command output fields and counters available in release 15.0.

None for this release.

**Deprecated P-GW Output Fields and Counters**

This section identifies deprecated P-GW output fields and counters that are no longer supported in release 15.0.

None for this release.
Chapter 19
SAEGW Changes in Release 15.0

This chapter identifies features and functionality added to, modified for, or deprecated from 15.0 SAEGW 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:

- September 30, 2013, added bulk statistics under New in the SAEGW Schema
SAEGW Enhancements for February 27, 2015

There are no SAEGW enhancements for this release.
SAEGW Enhancements for October 31, 2014

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
- ADC Enhancements
- CF Enhancements
- ECS Enhancements
- Firewall Enhancements
- GTPP Enhancements
- Lawful Intercept Enhancements
- InTracer Enhancements
- MVG Enhancements
- NAT Enhancements
- SNMP MIB Enhancements
- System & Platform Enhancements

---

**CSCun35216 - S4 to Gn SGSN HO, CCR-u shows RAT type event for UTRAN**

**Feature Changes**

**Behavior Change for S4-SGSN to GGSN Handover**

The fix for CSCun35216 has resulted in a behavior change.

**Previous Behavior:** In an S4-SGSN to GGSN handover, when there was no change in RAT change, a RAT change was getting detected.

**New Behavior:** In an S4-SGSN to GGSN handover, when there is no change in RAT change, then a RAT change will not be detected.
CSCup67356 - Rule failure counters not incremented

Feature Changes

Enhanced Output for show active-charging service statistics

The fix for CSCup67356 has resulted in a behavior change.

Previous Behavior: In the output for the show active-charging service statistics CLI command, the ACS reject reason for no active rule was not shown.

New Behavior: The show active-charging service statistics CLI command now indicates the number of calls rejected due to no active rule.

Performance Indicator Changes

show active-charging service statistics

The output of this command has been enhanced to indicate the number of calls rejected due to no active rule.

- ACS Reject Reason
- No Active rule in Subs:

CSCuq25059 - Assertion failure at sess/smgr/sessmgr_ggsn.c:25058

Feature Changes

Behavior Change for Unknown Traffic Type Passed to GGSN

The fix for CSCuq25059 has resulted in a behavior change.

Previous Behavior: A traffic type other than 1,2,3,4 in the Create PDP Req message would result in a crash at the GGSN.

New Behavior: If an unknown traffic type (that is, other than 1,2,3,4) is passed to the GGSN it will be mapped to a QCI corresponding to background class and will not result in a crash.
SAEGW Enhancements for November 30, 2013

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
- ADC Enhancements
- CF Enhancements
- ECS Enhancements
- Firewall Enhancements
- GTPP Enhancements
- Lawful Intercept Enhancements
- InTracer Enhancements
- MVG Enhancements
- NAT Enhancements
- SNMP MIB Enhancements
- System & Platform Enhancements

---

**CSCui79823 - Customer ENT LAB- Tracfone local issue for iRat from 4G to S4**

**Feature Changes**

**APN-AMBR in Local Policy Rule Matching**

The value was passed to local policy and rule matching was done only after the APN-AMBR values were received in the Modify Bearer Request.

Completed changes to copy the APN-AMBR values from the clp. It is used when the value is not received from the Modify Bearer Request.

**Previous Behavior**: During 4G to S4-SGSN handoff, APN-AMBR will not be sent; therefore, APN-AMBR rules fail in local policy.
New Behavior: For 4G to S4-SGSN handoff, previously used APN-AMBR will be used in local policy rule matching.
SAEGW Enhancements for September 30, 2013

SAEGW Feature Changes as of September 30, 2013

This section provides information on SAEGW feature changes in release 15.0.

**Important:** For more information regarding features in this section, refer to the *SAEGW Administration Guide* for this release.

### New SAEGW Features

This section identifies new SAEGW features available in release 15.0.

**Authorized Qos Policy to be Displayed at SM for P-GW and SAEGW**

Code added to display PCRF authorized in `show subscribers pgw-only full all` for P-GW and in `show subscribers saegw-only full all` for SAEGW.

**Node Functionality GTP Echo**

This feature helps exchange capabilities of two communicating GTP nodes, and uses the new feature based on whether it is supported by the other node.

This feature allows S-GW to exchange its capabilities (MABR, PRN, NTSR) with the peer entities through ECHO messages. By this, if both the peer nodes support some common features, then they can make use of new messages to communicate with each other.

With new “node features” IE support in ECHO request/response message, each node can send its supported features (MABR, PRN, NTSR). This way, S-GW can learn the peer node’s supported features. S-GW’s supported features can be configured by having some configuration at the service level.

If S-GW wants to use new message, such as P-GW Restart Notification, then S-GW should check if the peer node supports this new feature or not. If the peer does not support it, then S-GW should fall back to old behavior.

If S-GW receives a new message from the peer node, and if S-GW does not support this new message, then S-GW should ignore it. If S-GW supports the particular feature, then it should handle the new message as per the specification.

### Modified SAEGW Features

This section identifies SAEGW features modified in release 15.0.

**3GPP TS 29.281 (GTP-U) Release 10 Compliance**

**Previous Behavior:** P-GW was not fully compliant to 3GPP TS 29.281 Rel-10 to support UDP Port Extension header in Error indication message and Supported Extension Headers Notification message.

**New Behavior:** This feature enhances the GTP-U capabilities of P-GW in compliance to 3GPP TS 29.281 Rel-10. Support for UDP Port Extension Header in Error Indication message and Supported Extension Headers Notification message was added to become fully compliant with 3GPP Release 10.
Supported Extension Headers Notification message indicates a list of supported extension headers that the node can support. This message is sent only in case a GTP entity was required to interpret a mandatory extension header (by setting the comprehension required in extension header), but the GTP entity was not yet upgraded to support that extension header.

- If a Supported Extension Headers Notification is received from peer GTP-U entity, node will not send the extension header to the peer entity.
- If a message which contains extension header is received from peer GTP-U entity and the extension header is set to comprehension required and the extension header cannot be interpreted by the node, it will send a Supported Extension Headers Notification message. This message shall include all the extension headers supported by the node.

UDP Port Extension header helps in handling the Error-Indication message efficiently. If any GTP-U peer supports this extension header, then sending this extension header in Error-Indication message will help in processing the Error-Indication message.

Support for Supported Extension Headers Notification message helps notify the GTP-U peer about the GT-U capabilities of the node. This message is sent only in case the node was required to interpret a mandatory extension header (by setting the comprehension required in extension header), but the node was not yet upgraded to support that extension header.

**DSCP Marking - GTP-U on per APN Basis**

This feature provides the flexibility to have a different DSCP marking table on per APN basis so that traffic on each of the APNs can be marked differently, depending on the needs of the APN.

The P-GW supports configurable DSCP marking of the outer header of a GTP-U tunnel packet based on a QCI/THP table for the S5/S8 and Gn/Gp interfaces. This feature allows configuring DSCP marking table on a per APN basis.

Previously, DSCP marking table was configured on P-GW service level. As part of this requirement, new CLI is added to associate the qos-qci-mapping table in APN.

In order to be backward compatible with old configuration, if a DSCP marking table is associated with P-GW service and not with the APN, then the one in P-GW service will be used. If table is associated in both P-GW service and APN, then the one on APN will take precedence.

**Indirect Forward Tunneling - DL and UL Forwarding**

Support is provided for LTE to 3G PS Handovers with downlink and uplink indirect data forwarding in this release.

**SRVCC PS-to-CS Handover Indication Support in P-GW**

This feature helps in notifying the PCRF about the exact reason for PCC rule deactivation on Voice bearer deletion. This exact cause will help PCRF to then take further action appropriately.

**Previous Behavior:**

1. Support of voice bearer flag in BearerFlags IE was not present in Delete Bearer Cmd initiated by MME.
2. Support of new Rule Failure Code PS_TO_CS_HANOVER in Charging Rule Report was not present.

**New Behavior:** This feature ensures complete compliance for SRVCC, including support for PS-to-CS handover indication when voice bearers are released. The support for SRVCC feature was first added in StarOS Release 12.2.

SRVCC service for LTE comes into the picture when a single radio User Equipment (UE) accessing IMS-anchored voice call services switches from the LTE network to the Circuit Switched domain while it is able to transmit or receive on only one of these access networks at a given time. This removes the need for a UE to have multiple Radio Access Technology (RAT) capability.
SAEGW Changes in Release 15.0

1. After handing over the PS sessions to the target, the source MME shall remove the voice bearers by deactivating the voice bearer(s) towards S-GW/P-GW and setting the VB (Voice Bearer) flag of Bearer Flags IE in the Delete Bearer Command message (TS 29.274 v9.5.0).
2. If the IP-CAN bearer termination is caused by the PS to CS handover, the PCEF may report related PCC rules for this IP-CAN bearer by including the Rule-Failure-Code AVP set to the value PS_TO_CS_HANDOVER (TS 29.212 v10.2.0 and TS 23.203 v10.3.0).

Support for new AVP PS-to-CS-Session-Continuity (added in 3GPP Release 11) inside Charging Rule Install, which indicates if the bearer is selected for PS to CS continuity is not added.

SAEGW Command Changes as of September 30, 2013

This section provides information on SAEGW command changes in release 15.0.

Important: For more information regarding commands in this section, refer to the Command Line Interface Reference for this release.

New SAEGW Commands

This section identifies new SAEGW commands available in release 15.0.

description

The following new command configures a short description for the specified peer profile.

```
configure

    peer-profile service-type { pgw-access | sgw-network } { default | name profile_name }
    [ -noconfirm ]

    description description

    no description

    end
```

gtpc

The following new command configures the GTP-C settings for the specified peer profile.

```
configure

    peer-profile service-type { pgw-access | sgw-network } { default | name profile_name }
    [ -noconfirm ]

    gtpc { echo { interval seconds | retransmission-timeout seconds } | max-retransmissions number | retransmission-timeout seconds }

    default gtpc { echo [ interval | retransmission-timeout ] | max-retransmissions | retransmission-timeout }

    no gtpc echo
```
end

Notes:

- `gtpc echo interval seconds` must be an integer from 60 to 3600. Default: 60
- `gtpc echo retransmission-timeout seconds` must be an integer from 1 to 20.
  
  Default: 5
- `gtpc max-retransmissions number` must be an integer from 0 to 15.
  
  Default: 4
- `gtpc retransmission-timeout seconds` must be an integer from 1 to 20.
  
  Default: 5

peer-map

The following new command creates a peer map and enters the Peer Map Configuration mode. This new command mode enables the operator to map and LTE Policy to a peer profile based on matching criteria and precedence for the criteria.

```
configure
    lte-policy
        peer-map map_name [ -noconfirm ]
    no peer-map map_name
end
```

peer-profile

The following command creates a P-GW or S-GW peer profile and enters the Peer Profile Configuration mode.

```
configure
    peer-profile service-type { pgw-access | sgw-network } { default | name profile_name }
    [ -noconfirm ]
    no peer-profile service-type { pgw-access | sgw-network } name profile_name
end
```

Note:

- A maximum of 64 peer profiles can be configured.

precedence

The following new command configures the matching criteria and precedence for mapping an LTE Policy with a peer profile.

```
configure
    lte-policy
```

Cisco ASR 5x00 Release Change Reference
peer-map map_name [ -noconfirm ]

precedence priority match-criteria { all peer-profile-name profile_name | peer-ip-address { ip_address | ip_address/mask } [ serving-plmnid mcc mnc mnc ] peer-profile-name profile_name | serving-plmnid mcc mnc mnc [ peer-ip-address { ip_address | ip_address/mask } ] peer-profile-name profile_name }

no precedence priority

doc

Notes:

- Precedence 1 has highest priority.
  
- priority must be an integer from 1 to 1024.
  
- A maximum of 1024 precedence entries can be configured.

- To map a peer to a profile when there is no specific criteria required, use the all keyword.
  
- mcc must be a three-digit number between 100 and 999.

- mnc must be a two- or three-digit number between 00 and 999.

show peer-profile

The following new command displays configuration of the specified peer profile.

```
show peer-profile { all | full { all | name profile_name } | name profile_name }
```

Modified SAEGW Commands

This section identifies SAEGW commands modified in release 15.0.

associate

The new keyword peer-map associates an LTE Policy peer map with a P-GW or S-GW service.

```
configure

context context_name

{ pgw-service | sgw-service } svc_name

associate peer-map map_name

no associate peer-map

end
```

associate

The new keyword qci-qos-mapping has been added to configure DSCP marking of the outer header of a GTP-U tunnel packet based on a QCI table. DSCP marking shall be supported on a per APN basis.

```
configure
```
context context_name
  apn apn_name
    qci-qos-mapping table_name
    no qci-qos-mapping
  end

show lte-policy peer-map

The new keyword peer-map displays configuration of the specified LTE Policy peer map.

show lte-policy peer-map { name map_name | summary }

Deprecated SAEGW Commands

This section identifies deprecated SAEGW commands that are no longer supported in release 15.0.
None for this release.

SAEGW Performance Indicator Changes as of September 30, 2013

This section provides information on SAEGW performance indicator changes in release 15.0.

Important: For more information regarding bulk statistics and output fields and counters in this section, refer to the Statistics and Counters Reference for this release.

New SAEGW Bulk Statistics

This section identifies new SAEGW bulk statistics available in release 15.0.

Important: For more information regarding bulk statistics and output fields and counters in this section, refer to the Statistics and Counters Reference for this release.

New in the SAEGW Schema

The following bulkstats have been added for S-GW restoration:

- pgw-sesststat-sgwrstr-inrstrstate
- pgw-sesststat-sgwrstr-recovered
- pgw-sesststat-sgwrstr-released
- pgw-sesststat-sgwrstr-uplpktdrop
- pgw-sesststat-sgwrstr-uplbkbytedrop
- pgw-sesststat-sgwrstr-dnlkpktdrop
- pgw-sessstat-sgwrstr-dnlkbytedrop

**Corrected Content:** This section includes corrections to previously published content. The previous content stated that, “Overcharging Protection functionality has been implemented as lab quality”, which is incorrect. Overcharging Protection functionality has been implemented as deploy quality.

The following bulkstats have been added for overcharging protection:

- pgw-sessstat-ovrchrgprtcnt-uplkpktdrop
- pgw-sessstat-ovrchrgprtcnt-uplkbytedrop
- pgw-sessstat-ovrchrgprtcnt-dnlkpktdrop
- pgw-sessstat-ovrchrgprtcnt-dnlkbytedrop

The following bulkstats have been added:

- sgw-sessstat-totcur-pdn-paused-charging
- pgw-sessstat-bearrel-nwded4sgsn
- saegw-ipv4-colocated-pdn-dl-packets
- saegw-ipv4-colocated-pdn-dl-bytes
- saegw-ipv4-colocated-pdn-ul-packets
- saegw-ipv4-colocated-pdn-ul-bytes
- saegw-ipv6-colocated-pdn-dl-packets
- saegw-ipv6-colocated-pdn-dl-bytes
- saegw-ipv6-colocated-pdn-ul-packets
- saegw-ipv6-colocated-pdn-ul-bytes
- saegw-ipv4v6-colocated-pdn-ipv4-dl-packets
- saegw-ipv4v6-colocated-pdn-ipv4-dl-bytes
- saegw-ipv4v6-colocated-pdn-ipv4-ul-packets
- saegw-ipv4v6-colocated-pdn-ipv4-ul-bytes
- saegw-ipv4v6-colocated-pdn-ipv6-dl-packets
- saegw-ipv4v6-colocated-pdn-ipv6-dl-bytes
- saegw-ipv4v6-colocated-pdn-ipv6-ul-packets
- saegw-ipv4v6-colocated-pdn-ipv6-ul-bytes
- saegw-ipv4-sgw_anchored-pdn-dl-packets
- saegw-ipv4-sgw_anchored-pdn-dl-bytes
- saegw-ipv4-sgw_anchored-pdn-ul-packets
- saegw-ipv4-sgw_anchored-pdn-ul-bytes
- saegw-ipv6-sgw_anchored-pdn-dl-packets
- saegw-ipv6-sgw_anchored-pdn-dl-bytes
- saegw-ipv6-sgw_anchored-pdn-ul-packets
- saegw-ipv6-sgw_anchored-pdn-ul-bytes
- saegw-ipv6-sgw_anchor-pdn-ul-bytes
- saegw-ipv4v6-sgw_anchor-pdn-ipv4-dl-packets
- saegw-ipv4v6-sgw_anchor-pdn-ipv4-dl-bytes
- saegw-ipv4v6-sgw_anchor-pdn-ipv4-ul-packets
- saegw-ipv4v6-sgw_anchor-pdn-ipv4-ul-bytes
- saegw-ipv4v6-sgw_anchor-pdn-ipv6-dl-packets
- saegw-ipv4v6-sgw_anchor-pdn-ipv6-dl-bytes
- saegw-ipv4v6-sgw_anchor-pdn-ipv6-ul-packets
- saegw-ipv4v6-sgw_anchor-pdn-ipv6-ul-bytes
- saegw-ipv4-pgw_anchor-pdn-dl-packets
- saegw-ipv4-pgw_anchor-pdn-dl-bytes
- saegw-ipv4-pgw_anchor-pdn-ul-packets
- saegw-ipv4-pgw_anchor-pdn-ul-bytes
- saegw-ipv6-pgw_anchor-pdn-dl-packets
- saegw-ipv6-pgw_anchor-pdn-dl-bytes
- saegw-ipv6-pgw_anchor-pdn-ul-packets
- saegw-ipv6-pgw_anchor-pdn-ul-bytes
- saegw-ipv4v6-pgw_anchor-pdn-ipv4-dl-packets
- saegw-ipv4v6-pgw_anchor-pdn-ipv4-dl-bytes
- saegw-ipv4v6-pgw_anchor-pdn-ipv4-ul-packets
- saegw-ipv4v6-pgw_anchor-pdn-ipv4-ul-bytes
- saegw-ipv4v6-pgw_anchor-pdn-ipv6-dl-packets
- saegw-ipv4v6-pgw_anchor-pdn-ipv6-dl-bytes
- saegw-ipv4v6-pgw_anchor-pdn-ipv6-ul-packets
- saegw-ipv4v6-pgw_anchor-pdn-ipv6-ul-bytes
- saegw-ipv4-ggsn-pdn-dl-packets
- saegw-ipv4-ggsn-pdn-dl-bytes
- saegw-ipv4-ggsn-pdn-ul-packets
- saegw-ipv4-ggsn-pdn-ul-bytes
- saegw-ipv6-ggsn-pdn-dl-packets
- saegw-ipv6-ggsn-pdn-dl-bytes
- saegw-ipv6-ggsn-pdn-ul-packets
- saegw-ipv6-ggsn-pdn-ul-bytes
- saegw-ipv4v6-ggsn-pdn-ipv4-dl-packets
- saegw-ipv4v6-ggsn-pdn-ipv4-dl-bytes
- saegw-ipv4v6-ggsn-pdn-ipv4-ul-packets
- saegw-ipv4v6-ggsn-pdn-ipv4-ul-bytes
- saegw-ipv4v6-ggsn-pdn-ipv6-dl-packets
- saegw-ipv4v6-ggsn-pdn-ipv6-dl-bytes
- saegw-ipv4v6-ggsn-pdn-ipv6-ul-packets
- saegw-ipv4v6-ggsn-pdn-ipv6-ul-bytes
- saegw-ggsn-sessstat-bearact-emergency-def
- saegw-ggsn-sessstat-bearact-emergency-auth-imsi-def
- saegw-ggsn-sessstat-bearact-emergency-unauth-imsi-def
- saegw-ggsn-sessstat-bearact-emergency-only-imei-def
- saegw-ggsn-sessstat-bearact-ue-init-ded
- saegw-ggsn-sessstat-bearact-nw-init-ded
- saegw-ggsn-sessstat-bearact-emergency-ded
- saegw-ggsn-sessstat-bearact-emergency-auth-imsi-ded
- saegw-ggsn-sessstat-bearact-emergency-unauth-imsi-ded
- saegw-ggsn-sessstat-bearact-emergency-only-imei-ded
- saegw-ggsn-sessstat-bearact-nw-init-ded-att
- saegw-ggsn-sessstat-bearset-emergency-def
- saegw-ggsn-sessstat-bearset-emergency-auth-imsi-def
- saegw-ggsn-sessstat-bearset-emergency-unauth-imsi-def
- saegw-ggsn-sessstat-bearset-emergency-only-imei-def
- saegw-ggsn-sessstat-bearset-ue-init-ded
- saegw-ggsn-sessstat-bearset-nw-init-ded
- saegw-ggsn-sessstat-bearset-emergency-ded
- saegw-ggsn-sessstat-bearset-emergency-auth-imsi-ded
- saegw-ggsn-sessstat-bearset-emergency-unauth-imsi-ded
- saegw-ggsn-sessstat-bearset-emergency-only-imei-ded
- saegw-ggsn-sessstat-bearrel-nwdefadmin
- saegw-ggsn-sessstat-bearrel-nwdefgtp
- saegw-ggsn-sessstat-bearrel-nwdefsgw
- saegw-ggsn-sessstat-bearrel-nwdef54sgsn
- saegw-ggsn-sessstat-bearrel-nwdefmme
- saegw-ggsn-sessstat-bearrel-nwdedadmin
• saegw-ggsn-sessstat-bearrel-nwedgtp
• saegw-ggsn-sessstat-bearrel-nweddmme
• saegw-ggsn-sessstat-bearrel-nweddefbear
• saegw-ggsn-sessstat-bearrel-nwedgdxdisc
• saegw-ggsn-sessstat-bearrel-nweds4sgsn
• saegw-ggsn-sessstat-bearrelfail-def
• saegw-ggsn-sessstat-bearrelfail-ded
• saegw-ggsn-sessstat-bearrej-def
• saegw-ggsn-sessstat-bearrej-ded
• saegw-ggsn-sessstat-bearrej-emergency-def
• saegw-ggsn-sessstat-bearrej-emergency-ded
• saegw-ggsn-sessstat-bearrej-nores
• saegw-ggsn-sessstat-bearrej-ureq
• saegw-ggsn-sessstat-bearrej-ureq-nores
• saegw-ggsn-sessstat-bearrej-misapn
• saegw-ggsn-sessstat-bearrej-nwreq
• saegw-ggsn-sessstat-bearrej-nwreq-nores
• saegw-ggsn-sessstat-bearrej-nwreq-nomem
• saegw-ggsn-sessstat-bearrej-nwreq-sysfail
• saegw-ggsn-sessstat-bearrej-apnmode
• saegw-ggsn-sessstat-bearrej-pdn
• saegw-ggsn-sessstat-bearrej-apnrestr
• saegw-ggsn-sessstat-bearrej-subsauth
• saegw-ggsn-sessstat-bearrej-subssaddrnotallow
• saegw-ggsn-sessstat-bearrej-subssaddrnotalloc
• saegw-ggsn-sessstat-bearrej-dynaddrnotalloc
• saegw-ggsn-sessstat-bearrej-subssaddrnotpres
• saegw-ggsn-sessstat-bearmod-ueinit
• saegw-ggsn-sessstat-bearmod-nwinit
• saegw-ggsn-sessstat-bearmod-ueqos
• saegw-ggsn-sessstat-bearmod-ueft
• saegw-ggsn-sessstat-bearmod-nwqos
• saegw-ggsn-sessstat-bearmod-nwft
• saegw-ggsn-sessstat-bearmodfail-ueinit
• saegw-ggsn-sessstat-bearmodfail-nwinit
• saegw-ggsn-sessstat-bearmodfail-uenores
• saegw-ggsn-sessstat-bearmodfail-uesemtft
• saegw-ggsn-sessstat-bearmodfail-uesyntft
• saegw-ggsn-sessstat-bearmodfail-uesempkt
• saegw-ggsn-sessstat-bearmodfail-uesynpkt
• saegw-ggsn-sessstat-bearmodfail-nwnores
• saegw-ggsn-sessstat-bearmodfail-nwnomem
• saegw-ggsn-sessstat-bearmodfail-nwsysfail
• saegw-ggsn-sessstat-bearmodfail-nwsemtft
• saegw-ggsn-sessstat-bearmodfail-nwsemtft
• saegw-ggsn-sessstat-bearmodfail-nwsempkt
• saegw-ggsn-sessstat-bearmodfail-nwsynpkt
• saegw-ggsn-sessstat-bearmodfail-qos-uenores
• saegw-ggsn-sessstat-bearmodfail-qos-uesemtft
• saegw-ggsn-sessstat-bearmodfail-qos-uesyntft
• saegw-ggsn-sessstat-bearmodfail-qos-uesempkt
• saegw-ggsn-sessstat-bearmodfail-qos-uesynpkt
• saegw-ggsn-sessstat-bearmodfail-qos-nwnores
• saegw-ggsn-sessstat-bearmodfail-qos-nwnomem
• saegw-ggsn-sessstat-bearmodfail-qos-nwsysfail
• saegw-ggsn-sessstat-bearmodfail-qos-nwsemtft
• saegw-ggsn-sessstat-bearmodfail-qos-nwsemtft
• saegw-ggsn-sessstat-bearmodfail-qos-nwsempkt
• saegw-ggsn-sessstat-bearmodfail-qos-nwsynpkt
• saegw-ggsn-sessstat-beardel-ded
• saegw-ggsn-sessstat-nw-init-qos-update-att
• saegw-ggsn-sessstat-nw-init-no-qos-update-att
• saegw-ggsn-sessstat-nw-init-bearer-fail-cause
• saegw-ggsn-sessstat-ipv4addaloc
• saegw-ggsn-sessstat-ipaddaloc-ipv4localpool
• saegw-ggsn-sessstat-ipaddaloc-ipv4staticaddr
• saegw-ggsn-sessstat-ipaddaloc-ipv4radaddr
• saegw-ggsn-sessstat-ipv6addaloc
<table>
<thead>
<tr>
<th>SAEGW Changes in Release 15.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAEGW Enhancements for September 30, 2013</td>
</tr>
</tbody>
</table>

- saegw-ggsn-sessstat-ipaddaloc-ipv6auto
- saegw-ggsn-subplmnstat-homesubact
- saegw-ggsn-subplmnstat-homesubsetup
- saegw-ggsn-subplmnstat-homesubrel
- saegw-ggsn-subplmnstat-roamsubact
- saegw-ggsn-subplmnstat-roamsubsetup
- saegw-ggsn-subplmnstat-roamsubrel
- saegw-ggsn-subplmnstat-visitsubact
- saegw-ggsn-subplmnstat-visitsubsetup
- saegw-ggsn-subplmnstat-visitsubrel
- saegw-ggsn-handoverstat-intersgsnatt
- saegw-ggsn-handoverstat-intersgsnsucc
- saegw-ggsn-handoverstat-intersgsnfail
- saegw-ggsn-handoverstat-gngptolteatt
- saegw-ggsn-handoverstat-gngptoltesucc
- saegw-ggsn-handoverstat-gngptoltefail
- saegw-ggsn-handoverstat-ltetogngpatt
- saegw-ggsn-handoverstat-ltetogngpsucc
- saegw-ggsn-handoverstat-ltetogngpfail
- saegw-ggsn-subqosstat-bearact-qci1
- saegw-ggsn-subqosstat-bearact-qci2
- saegw-ggsn-subqosstat-bearact-qci3
- saegw-ggsn-subqosstat-bearact-qci4
- saegw-ggsn-subqosstat-bearact-qci5
- saegw-ggsn-subqosstat-bearact-qci6
- saegw-ggsn-subqosstat-bearact-qci7
- saegw-ggsn-subqosstat-bearact-qci8
- saegw-ggsn-subqosstat-bearact-qci9
- saegw-ggsn-subqosstat-bearact-qcinongbr
- saegw-ggsn-subqosstat-bearact-qcigbr
- saegw-ggsn-subqosstat-bearset-qci1
- saegw-ggsn-subqosstat-bearset-qci2
- saegw-ggsn-subqosstat-bearset-qci3
- saegw-ggsn-subqosstat-bearset-qci4
- saegw-ggsn-subqosstat-bearset-qci5
- saegw-ggsn-subqosstat-bearset-qci6
- saegw-ggsn-subqosstat-bearset-qci7
- saegw-ggsn-subqosstat-bearset-qci8
- saegw-ggsn-subqosstat-bearset-qci9
- saegw-ggsn-subqosstat-bearset-qcinongbr
- saegw-ggsn-subqosstat-bearset-qcigbr
- saegw-ggsn-subqosstat-bearrel-qci1
- saegw-ggsn-subqosstat-bearrel-qci2
- saegw-ggsn-subqosstat-bearrel-qci3
- saegw-ggsn-subqosstat-bearrel-qci4
- saegw-ggsn-subqosstat-bearrel-qci5
- saegw-ggsn-subqosstat-bearrel-qci6
- saegw-ggsn-subqosstat-bearrel-qci7
- saegw-ggsn-subqosstat-bearrel-qci8
- saegw-ggsn-subqosstat-bearrel-qci9
- saegw-ggsn-subqosstat-bearrel-qcinongbr
- saegw-ggsn-subqosstat-bearrel-qcigbr
- saegw-ggsn-subdatatstat-totulpktfwd
- saegw-ggsn-subdatatstat-ulpktfwd-qci1
- saegw-ggsn-subdatatstat-ulpktfwd-qci2
- saegw-ggsn-subdatatstat-ulpktfwd-qci3
- saegw-ggsn-subdatatstat-ulpktfwd-qci4
- saegw-ggsn-subdatatstat-ulpktfwd-qci5
- saegw-ggsn-subdatatstat-ulpktfwd-qci6
- saegw-ggsn-subdatatstat-ulpktfwd-qci7
- saegw-ggsn-subdatatstat-ulpktfwd-qci8
- saegw-ggsn-subdatatstat-ulpktfwd-qci9
- saegw-ggsn-subdatatstat-ulpktfwd-stdqcinongbr
- saegw-ggsn-subdatatstat-ulpktfwd-stdqcigbr
- saegw-ggsn-subdatatstat-ulpktfwd-qcinongbr
- saegw-ggsn-subdatatstat-ulpktfwd-qcigbr
- saegw-ggsn-subdatatstat-ulpktfwd-totgbr
- saegw-ggsn-subdatatstat-ulpktfwd-totnongbr
• saegw-ggsn-subdatastat-totulbytefwd
• saegw-ggsn-subdatastat-ulbytefwd-qci1
• saegw-ggsn-subdatastat-ulbytefwd-qci2
• saegw-ggsn-subdatastat-ulbytefwd-qci3
• saegw-ggsn-subdatastat-ulbytefwd-qci4
• saegw-ggsn-subdatastat-ulbytefwd-qci5
• saegw-ggsn-subdatastat-ulbytefwd-qci6
• saegw-ggsn-subdatastat-ulbytefwd-qci7
• saegw-ggsn-subdatastat-ulbytefwd-qci8
• saegw-ggsn-subdatastat-ulbytefwd-qci9
• saegw-ggsn-subdatastat-ulbytefwd-stdqcinongbr
• saegw-ggsn-subdatastat-ulbytefwd-stdqcigbr
• saegw-ggsn-subdatastat-ulbytefwd-qqinongbr
• saegw-ggsn-subdatastat-ulbytefwd-qqigbr
• saegw-ggsn-subdatastat-ulbytefwd-totgbr
• saegw-ggsn-subdatastat-ulbytefwd-totnongbr
• saegw-ggsn-subdatastat-totdlpktfwd
• saegw-ggsn-subdatastat-dlpktfwd-qci1
• saegw-ggsn-subdatastat-dlpktfwd-qci2
• saegw-ggsn-subdatastat-dlpktfwd-qci3
• saegw-ggsn-subdatastat-dlpktfwd-qci4
• saegw-ggsn-subdatastat-dlpktfwd-qci5
• saegw-ggsn-subdatastat-dlpktfwd-qci6
• saegw-ggsn-subdatastat-dlpktfwd-qci7
• saegw-ggsn-subdatastat-dlpktfwd-qci8
• saegw-ggsn-subdatastat-dlpktfwd-qci9
• saegw-ggsn-subdatastat-dlpktfwd-stdqcinongbr
• saegw-ggsn-subdatastat-dlpktfwd-stdqcigbr
• saegw-ggsn-subdatastat-dlpktfwd-qqinongbr
• saegw-ggsn-subdatastat-dlpktfwd-qqigbr
• saegw-ggsn-subdatastat-dlpktfwd-totgbr
• saegw-ggsn-subdatastat-dlpktfwd-totnongbr
• saegw-ggsn-subdatastat-totdlbytefwd
• saegw-ggsn-subdatastat-dlbytefwd-qci1
- saegw-ggsn-subdatastat-dlbytefwd-qci2
- saegw-ggsn-subdatastat-dlbytefwd-qci3
- saegw-ggsn-subdatastat-dlbytefwd-qci4
- saegw-ggsn-subdatastat-dlbytefwd-qci5
- saegw-ggsn-subdatastat-dlbytefwd-qci6
- saegw-ggsn-subdatastat-dlbytefwd-qci7
- saegw-ggsn-subdatastat-dlbytefwd-qci8
- saegw-ggsn-subdatastat-dlbytefwd-qci9
- saegw-ggsn-subdatastat-dlbytefwd-stdqcinongbr
- saegw-ggsn-subdatastat-dlbytefwd-stdqcigbr
- saegw-ggsn-subdatastat-dlbytefwd-qcinongbr
- saegw-ggsn-subdatastat-dlbytefwd-qcigbr
- saegw-ggsn-subdatastat-dlbytefwd-totgbr
- saegw-ggsn-subdatastat-dlbytefwd-totnongbr
- saegw-ggsn-subdatastat-totulpktdrop
- saegw-ggsn-subdatastat-ulpktdrop-qci1
- saegw-ggsn-subdatastat-ulpktdrop-qci2
- saegw-ggsn-subdatastat-ulpktdrop-qci3
- saegw-ggsn-subdatastat-ulpktdrop-qci4
- saegw-ggsn-subdatastat-ulpktdrop-qci5
- saegw-ggsn-subdatastat-ulpktdrop-qci6
- saegw-ggsn-subdatastat-ulpktdrop-qci7
- saegw-ggsn-subdatastat-ulpktdrop-qci8
- saegw-ggsn-subdatastat-ulpktdrop-qci9
- saegw-ggsn-subdatastat-ulpktdrop-stdqcinongbr
- saegw-ggsn-subdatastat-ulpktdrop-stdqcigbr
- saegw-ggsn-subdatastat-ulpktdrop-qcinongbr
- saegw-ggsn-subdatastat-ulpktdrop-qcigbr
- saegw-ggsn-subdatastat-ulpktdrop-totgbr
- saegw-ggsn-subdatastat-ulpktdrop-totnongbr
- saegw-ggsn-subdatastat-totulbytedrop
- saegw-ggsn-subdatastat-ulpbytedrop-qci1
- saegw-ggsn-subdatastat-ulpbytedrop-qci2
- saegw-ggsn-subdatastat-ulpbytedrop-qci3
• saegw-ggsn-subdatastat-ulbytedrop-qci4
• saegw-ggsn-subdatastat-ulbytedrop-qci5
• saegw-ggsn-subdatastat-ulbytedrop-qci6
• saegw-ggsn-subdatastat-ulbytedrop-qci7
• saegw-ggsn-subdatastat-ulbytedrop-qci8
• saegw-ggsn-subdatastat-ulbytedrop-qci9
• saegw-ggsn-subdatastat-ulbytedrop-stdqcinongbr
• saegw-ggsn-subdatastat-ulbytedrop-stdqcigbr
• saegw-ggsn-subdatastat-ulbytedrop-qcinongbr
• saegw-ggsn-subdatastat-ulbytedrop-qcigbr
• saegw-ggsn-subdatastat-ulbytedrop-totgbr
• saegw-ggsn-subdatastat-ulbytedrop-totnongbr
• saegw-ggsn-subdatastat-totdlpktdrop
• saegw-ggsn-subdatastat-dlpktdrop-qci1
• saegw-ggsn-subdatastat-dlpktdrop-qci2
• saegw-ggsn-subdatastat-dlpktdrop-qci3
• saegw-ggsn-subdatastat-dlpktdrop-qci4
• saegw-ggsn-subdatastat-dlpktdrop-qci5
• saegw-ggsn-subdatastat-dlpktdrop-qci6
• saegw-ggsn-subdatastat-dlpktdrop-qci7
• saegw-ggsn-subdatastat-dlpktdrop-qci8
• saegw-ggsn-subdatastat-dlpktdrop-qci9
• saegw-ggsn-subdatastat-dlpktdrop-stdqcinongbr
• saegw-ggsn-subdatastat-dlpktdrop-stdqcigbr
• saegw-ggsn-subdatastat-dlpktdrop-qcinongbr
• saegw-ggsn-subdatastat-dlpktdrop-qcigbr
• saegw-ggsn-subdatastat-dlpktdrop-totgbr
• saegw-ggsn-subdatastat-dlpktdrop-totnongbr
• saegw-ggsn-subdatastat-totdlbytedrop
• saegw-ggsn-subdatastat-dlbytedrop-qci1
• saegw-ggsn-subdatastat-dlbytedrop-qci2
• saegw-ggsn-subdatastat-dlbytedrop-qci3
• saegw-ggsn-subdatastat-dlbytedrop-qci4
• saegw-ggsn-subdatastat-dlbytedrop-qci5
• saegw-ggsn-subdatastat-dlbytedrop-qci6
• saegw-ggsn-subdatastat-dlbytedrop-qci7
• saegw-ggsn-subdatastat-dlbytedrop-qci8
• saegw-ggsn-subdatastat-dlbytedrop-qci9
• saegw-ggsn-subdatastat-dlbytedrop-stdqcinongbr
• saegw-ggsn-subdatastat-dlbytedrop-stdqcigbr
• saegw-ggsn-subdatastat-dlbytedrop-qcinongbr
• saegw-ggsn-subdatastat-dlbytedrop-qcigbr
• saegw-ggsn-subdatastat-dlbytedrop-totgbr
• saegw-ggsn-subdatastat-dlbytedrop-totnongbr
• saegw-ggsn-subdatastat-totulpktdropmbrexc
• saegw-ggsn-subdatastat-ulpktdropmbrexc-qci1
• saegw-ggsn-subdatastat-ulpktdropmbrexc-qci2
• saegw-ggsn-subdatastat-ulpktdropmbrexc-qci3
• saegw-ggsn-subdatastat-ulpktdropmbrexc-qci4
• saegw-ggsn-subdatastat-ulpktdropmbrexc-qci5
• saegw-ggsn-subdatastat-ulpktdropmbrexc-qci6
• saegw-ggsn-subdatastat-ulpktdropmbrexc-qci7
• saegw-ggsn-subdatastat-ulpktdropmbrexc-qci8
• saegw-ggsn-subdatastat-ulpktdropmbrexc-qci9
• saegw-ggsn-subdatastat-ulpktdropmbrexc-stdqcinongbr
• saegw-ggsn-subdatastat-ulpktdropmbrexc-stdqcigbr
• saegw-ggsn-subdatastat-ulpktdropmbrexc-qcinongbr
• saegw-ggsn-subdatastat-ulpktdropmbrexc-qcigbr
• saegw-ggsn-subdatastat-ulpktdropmbrexc-totgbr
• saegw-ggsn-subdatastat-ulpktdropmbrexc-totnongbr
• saegw-ggsn-subdatastat-totulpktdropmbrexc
• saegw-ggsn-subdatastat-ulbytedropmbrexc-qci1
• saegw-ggsn-subdatastat-ulbytedropmbrexc-qci2
• saegw-ggsn-subdatastat-ulbytedropmbrexc-qci3
• saegw-ggsn-subdatastat-ulbytedropmbrexc-qci4
• saegw-ggsn-subdatastat-ulbytedropmbrexc-qci5
• saegw-ggsn-subdatastat-ulbytedropmbrexc-qci6
• saegw-ggsn-subdatastat-ulbytedropmbrexc-qci7
- saegw-ggsn-subdatastat-ulbytedropmbrexc-qci8
- saegw-ggsn-subdatastat-ulbytedropmbrexc-qci9
- saegw-ggsn-subdatastat-ulbytedropmbrexc-stdqcinongbr
- saegw-ggsn-subdatastat-ulbytedropmbrexc-stdq cigbr
- saegw-ggsn-subdatastat-ulbytedropmbrexc-qcinongbr
- saegw-ggsn-subdatastat-ulbytedropmbrexc-qcigbr
- saegw-ggsn-subdatastat-ulbytedropmbrexc-totgbr
- saegw-ggsn-subdatastat-ulbytedropmbrexc-totnongbr
- saegw-ggsn-subdatastat-totdlpktdropmbrexc
- saegw-ggsn-subdatastat-dlpktdropmbrexc-qci1
- saegw-ggsn-subdatastat-dlpktdropmbrexc-qci2
- saegw-ggsn-subdatastat-dlpktdropmbrexc-qci3
- saegw-ggsn-subdatastat-dlpktdropmbrexc-qci4
- saegw-ggsn-subdatastat-dlpktdropmbrexc-qci5
- saegw-ggsn-subdatastat-dlpktdropmbrexc-qci6
- saegw-ggsn-subdatastat-dlpktdropmbrexc-qci7
- saegw-ggsn-subdatastat-dlpktdropmbrexc-qci8
- saegw-ggsn-subdatastat-dlpktdropmbrexc-qci9
- saegw-ggsn-subdatastat-dlpktdropmbrexc-stdq cinongbr
- saegw-ggsn-subdatastat-dlpktdropmbrexc-stdq cigbr
- saegw-ggsn-subdatastat-dlpktdropmbrexc-qcinongbr
- saegw-ggsn-subdatastat-dlpktdropmbrexc-qcigbr
- saegw-ggsn-subdatastat-dlpktdropmbrexc-totgbr
- saegw-ggsn-subdatastat-dlpktdropmbrexc-totnongbr
- saegw-ggsn-subdatastat-totdlbytedropmbrexc
- saegw-ggsn-subdatastat-dlbytedropmbrexc-qci1
- saegw-ggsn-subdatastat-dlbytedropmbrexc-qci2
- saegw-ggsn-subdatastat-dlbytedropmbrexc-qci3
- saegw-ggsn-subdatastat-dlbytedropmbrexc-qci4
- saegw-ggsn-subdatastat-dlbytedropmbrexc-qci5
- saegw-ggsn-subdatastat-dlbytedropmbrexc-qci6
- saegw-ggsn-subdatastat-dlbytedropmbrexc-qci7
- saegw-ggsn-subdatastat-dlbytedropmbrexc-qci8
- saegw-ggsn-subdatastat-dlbytedropmbrexc-qci9
• saegw-ggsn-subdatastat-dlbytedropmbrexc-stdqcinongbr
• saegw-ggsn-subdatastat-dlbytedropmbrexc-stdqcigbr
• saegw-ggsn-subdatastat-dlbytedropmbrexc-qcinongbr
• saegw-ggsn-subdatastat-dlbytedropmbrexc-q cigbr
• saegw-ggsn-subdatastat-dlbytedropmbrexc-totgbr
• saegw-ggsn-subdatastat-dlbytedropmbrexc-totnongbr
• saegw-ggns-apnambratelim it-ulp ktdrop
• saegw-ggns-apnambratelim it-dlpktdrop
• saegw-ggns-apnambratelim it-ulbytedrop
• saegw-ggns-apnambratelim it-dlbytedrop

Modified SAEGW Bulk Statistics

This section identifies SAEGW bulk statistics modified in release 15.0.
None for this release.

Deprecated SAEGW Bulk Statistics

This section identifies deprecated SAEGW bulk statistics that are no longer supported in release 15.0.
None for this release.

New SAEGW Output Fields and Counters

This section identifies new SAEGW show command output fields and counters available in release 15.0.

show lte-policy peer-map name

The following fields display configuration information of the precedence entries within the specified LTE Policy peer map:
• Peer Map <name>
• precedence <n>

show peer-profile full all

The following fields display configuration information for all peer profiles:
• <service-type> Peer Profiles
• Peer Profile Name
• Description
• GTPC echo
• GTPC echo retransmission timeout
• GTPC echo interval
• GTPC max retransmissions
• GTPC retransmission timeout
• Lawful-intercept

**show session disconnect-reasons verbose**

The following new disconnect reason was added in support of SRVCC PS-to-CS handover indication:

• srvcc-ps-to-cs-handover(538)

**show subscribers pgw-only full all**

The following field has been added to display the peer profile for this subscriber:

• Network Peer Profile

**show subscribers saegw-only full all**

The following fields and counters have been added to display PCRF authorized QoS:

• PCRF Authorized Bearer QoS
  • QCI
  • ARP
    • PCI
    • PL
    • PVI
  • MBR Uplink(bps)
  • MBR Downlink(bps)
  • GBR Uplink(bps)
  • GBR Downlink(bps)
  • APN AMBR uplink
  • APN AMBR downlink

*Important:* This functionality has been implemented as lab quality.

**Modified SAEGW Output Fields and Counters**

This section identifies modified SAEGW show command output fields and counters available in release 15.0.

None for this release.

**Deprecated SAEGW Output Fields and Counters**

This section identifies deprecated SAEGW output fields and counters that are no longer supported in release 15.0.

None for this release.
Chapter 20
SGSN Changes in Release 15.0

This chapter identifies features and functionality added to, modified for, or deprecated from 15.0 SGSN software releases.
SGSN Enhancements for 15.0 MR6

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

---

**CSCur29374 - Service reject GMM cause 101 causing Service request loop**

**Feature Changes**

**GMM Cause Code for Service-reject in 3G is Modified**

**Previous Behavior:** In certain scenario's like service-requests arriving from different RAI or service-request during Inter-RAT at 2G and so on, the request is rejected with the GMM cause code “Message not compatible with the protocol state (101)”.

**New Behavior:** In above mentioned scenarios the service-reject is now sent with GMM cause code as “Implicitly detached (10)”.

**Customer Impact:** Non-compliant mobile subscribers will not loop the service-requests, as a result it is observed that the service-reject counter with GMM cause code “Message not compatible with the protocol state (101)” does not increase.
CSCur74184 - Global CN-ID should be sent in DirectInformationTransfer RIM with Iu-flex

Feature Changes

Including Global CN-ID in RANAP-RIM messages

When Iu-flex is activated, some RNCs may expect RIM information, issued by the SGSN, to include the Global CN-ID.

**Previous Behavior:** The SGSN does not include the Global CN-ID IE in the RANAP Direct Information Transfer message to the RNC.

**New Behavior:** When an RNC is configured as “pooled” as part of the SGSN’s IuPS Service configuration, then the SGSN includes the configured core network ID as the Global CN-ID IE in the RANAP Direct Information Transfer RIM messages towards the RNC.
SGSN Enhancements for October 31, 2014

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

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

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

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

---

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

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

---

**CSCu104175** - S4-SGSN to support R11 agreed CR to avoid SRVCC race condition

**Command Changes**

```bash
apn-type
```

New command, for both Gn-SGSN and S4-SGSN, in the APN profile can identify the type of APN as an IMS APN.

```bash
configure

    apn-profile profile_name

    apn-type ims

    remove apn-type ims
```

---

Cisco ASR 5x00 Release Change Reference
Notes:

- **apn-type ims** identifies the APN as an IMS APN. This enables the SGSN to delay sending Modify Bearer Request to the S-GW or Update PDP Context Request to the GGSN until after receiving the Forward Relocation Complete Ack from the peer during SRNS or handoff procedures. By default this identification is disabled.

- **remove** erases this identification configuration from the APN profile and resets to the default.

### CSCuo56840 - ’authenticate activate’ not working for 3G calls

**Feature Changes**

**‘authenticate activate’ Deprecated**

**Previous Behavior:** Authentication on activation was disabled/enabled in the configuration via CLI.

**New Behavior:** The SGSN no longer performs authentication on activation and this functionality has been removed from the CLI:

- The **authenticate all-events** CLI in the Call-Control Profile configuration mode no longer supports the SGSN’s authentication on activation.

- The **authenticate activate** command in the Call-Control Profile configuration mode, to enable/disable authentication on activation has been deprecated - see below.

**Command Changes**

**authenticate activate**

All forms of the **authenticate activate** command in the Call-Control Profile configuration mode have been deprecated.

```snippets
configure

call-control-profile profile_name

  authenticate activate [ access-type { gprs | umts } | first | frequency frequency | primary ] [ access-type { gprs | umts } ]

  [ no | remove ] authenticate activate [ access-type { gprs | umts } | first | primary ] [ access-type { gprs | umts } ]

end
```

**Performance Indicator Changes**

**show call-control-profile**
The output of the `show call-control-profile full name profile_name` no longer displays the following fields or any related values:

- Authentication Activate ANY (UMTS/GPRS)
- Authentication Activate UMTS
- Authentication Activate GPRS
- Authentication Activate First/Primary ANY (UMTS/GPRS)
- Authentication Activate First/Primary UMTS
- Authentication Activate First/Primary GPRS

### CSCuo86321 - issue with show subscriber and clear subscriber

#### Feature Changes

#### Evaluation of Idle-Time

The `show subscribers` and `clear subscribers` commands were not performing as expected when the `idle-time` keyword was included with the commands.

**Previous Behavior:** Evaluation of idle-time was based on MM signaling.

**New Behavior:** Evaluation of idle-time is now based on the data session idle time of the subscriber. The changes will result in:

- Both of the following commands will display the same number of subscribers based on the idle time calculation:
  
  - `show sub summary idle-time greater-than 1 | grep T`
  
  - `show sub idle-time greater-than 1`

- The following command functions are in sync so that clearing does not occur if the show command indicates no subscribers are found:
  
  - `show subscribers pan <panama> idle-time greater-than <number>`
  
  - `clear subscribers pan <panama> idle-time greater-than <number>`

- Yes/No confirmation has been added to the `clear subscribers apn <apn_name> idle-time greater-than <number>` to ensure subscribers are not accidentally cleared.

### CSCuo93431 - PDP failure due to subscribers stuck in disconnecting state

#### Feature Changes

#### Changes to Deactivation Procedures for Duplicate PDP Context

**Previous Behavior:** When the SGSN received a duplicate PDP (primary or secondary) Context Activation Request against a PDP (primary or secondary) context currently under deactivation, then the SGSN does not honor the duplicate Activate Request (primary or secondary) and replies with by sending an SM-STATUS (with cause message ‘not compatible with protocol state’).
**New Behavior:** The following defines how the SGSN now handles a duplicate *primary* Activation Request received during deactivation of a duplicate PDP context:

- if the new (duplicate) Activation Request is a primary and if the duplicate PDP context is a primary/bundle PDP context or a secondary PDP context, then the deactivation PDP context procedure continues and completes before the new primary PDP activation proceeds.

Note that the behavior has not changed if the new (duplicate) Activation Request is secondary and:

- If the duplicate PDP context is primary, then the new (duplicate) PDP Activation Request is rejected.
- If the duplicate PDP context is secondary and also the bundle is under deactivation, then the SGSN sends SM-STATUS.
- If the duplicate PDP context is secondary, then the deactivation completes and the new secondary PDP Activation Request is processed.

Note that ‘deactivation complete’ means the PDP context cleanup has occurred locally and disassociated the DPC towards the GGSN.

**Impact on Customer:** Duplicate PDP Activation Requests will be processed and sessions will be established by contacting the GGSN identified in the PDP Activation Requests received during the deactivation stage.

---

**CSCup14871 - Addition of logs/stats to analyze the call distribution issue.**

**Feature Changes**

**Analyzing Call Distribution Issues**

**New Behavior:** New statistics were added for internal debugging purposes. These statistics are not available for customer use.

**CSCup23087, CSCup94308 - Assertion failure with Invalid/unhandled event PMM_EVT_SM_INC_HO_COMP**

**Feature Changes**

**Reaction to RNC Overload during SRNS**

**New Behavior:** The RNC overload-action functionality has been enhanced so that it is now possible to configure the SGSN to reject SRNS (RANAP Relocation-Required and GTP Forward-Relocation Request messages) if the target RNC is in overload at a specified traffic level. This keyword setting is effective for both Inter-SGSN SRNS and Intra-SGSN SRNS.

will be rejected by SGSN if the target RNC is overloaded.

**Command Changes**

overload-action disable srns
The `overload-action disable` command has been enhanced to cause the SGSN to reject/disable SRNS if the RNC reaches overload.

```plaintext
configure

    context context_name

    iups-service service_name

    rnc id rnc_id

    overload-action disable { activate | attach | auth-challenge | modify-request | paging-downlink-data | ptmsi-reallocation | service-request-data | sms | srns }

    traffic-level traffic-level

    [ no | default ] overload-action disable { activate | attach | auth-challenge | modify-request | paging-downlink-data | ptmsi-reallocation | service-request-data | sms | srns }

end
```

Notes:

- `traffic-level` - Must be an integer from 1 to 15; default 15 for SRNS.

**Performance Indicator Changes**

**show gmm-statistics**

In support of the new RNC overload functionality, the `show gmm-statistics` command output displays a new counter type under subsection ‘Forward Relocation Reject Causes’

- Target RNC is overloaded

**show gmm-sm statistics**

As part of the new RNC Overload functionality, a new counter under CSCup94308 has been added for ‘Rnc Overload’ statistics in the output to count the number of SRNS calls rejected due to target RNC overload.

- Dropped SRNS relocations

**show iups-service**

The RNC overload traffic level for (inter/intra) SGSN SRNS is indicated with the new field:

- Srns: Disabled level 15

**CSCup34047 - Additional checks/logs to find the trigger for Wrong DNS query**

**Feature Changes**

**Additional Logs for DNS Query**
New Behavior: New log event (unusual) in DNS failure path for inter-SGSN RAU and Attach has been added. Logs now indicate old RA in RAU/Attach received from UE and DNS query string in the case of negative DNS response.

CSCup34085 - Sgtpcmgr high ErrIn may cause rx drop and path failure after demux migration

Feature Changes

Auto Syncing the GTP Echo Request

When the SGSN’s SGTPC-Mgr (GTP service) restarts, then the GTP path management procedures are restarted after the recovery, which can cause a drift in the Echo Request transmission time. As a result, the Echo Request initiated by the SGSN can be out of sync with the Echo Request initiated by the peer (GGSN/RNC) node. After this, if GTP Path failure occurs, then both nodes would detect it with a delay (the drift time).

Old Behavior: The GTP echo was transmittal only at echo intervals and upon expiry of retransmission timers.

New Behavior: This behavior change and associated CLI changes (see below) resolve the drift in Echo Request transmission by synchronizing the Echo Request with the peer node after GTP service restart. After recovery, when the SGSN receives the first Echo Request from the peer node, in addition to replying back with the Echo Response, the SGSN sends an Echo Request and restarts the associated timers.

NOTE:
- Both peer nodes using GTP Path management are assumed to have the same Retry Count and Retransmission Interval.
- This change in functionality is applicable to both GTPU and GTPC Path Management on the Gn/Gp and Iu-PS interfaces.
- This change in functionality avoids the drift in Echo Request (that may have happened) due to SGTPC-Mgr restart.

Command Changes

```
gtpc
```

A new keyword (`sync-echo-with-peer`) enables the SGSN to synchronize path management procedures with the peer, after GTP service restart.

```
configure

    context context_name

    sgtp-service service_name

    gtpc sync-echo-with-peer

[ no ] gtpc sync-echo-with-peer

end
```

Notes:
• Enabled is the default value.

gtpu

A new keyword (sync-echo-with-peer) enables the SGSN to synchronize path management procedures with the peer, after GTP service restart.

```
configure

context context_name

   sgtp-service service_name

       gtpu sync-echo-with-peer

       [ no ] gtpu sync-echo-with-peer

   end

Notes:
• Enabled is the default value.
```

gtpu

A new keyword (sync-echo-with-peer) enables the SGSN to synchronize path management procedures with the peer, after GTP service restart.

```
configure

context context_name

   iups-service service_name

       gtpu sync-echo-with-peer

       [ no ] gtpu sync-echo-with-peer

   end

Notes:
• Enabled is the default value.
```

**Performance Indicator Changes**

**show sgtp-service**

New fields have been added to the output of these show commands to illustrate the configuration for this functionality; whether it is enabled or disabled:

• GTP-C Sync Echo with Peer : Enabled/Disabled
• GTP-U Sync Echo with Peer : Enabled/Disabled
show iups-service

New fields have been added to the output of these show commands to illustrate the configuration for this functionality; whether it is enabled or disabled:

- **GTP-U Sync Echo with Peer**: Enabled/Disabled

**CSCup94785, CSCuq34454 - QOS management for uplink data messages in 2G**

**Feature Changes**

**ARP-RP Mapping for Radio Priority in Messages**

**Previous Behavior**: Radio priority was hardcoded to 4 irrespective of ARP values received by the SGSN from either a GGSN or an HLR. No mapping CLI existed for ARP and RP values in the SGSN configuration so radio priority of 4 was sent in the following downlink signaling messages:

- Activate PDP Accept.
- Modify PDP Request during network initiated PDP modification procedure.
- Modify PDP Accept during MS initiated PDP modification procedure provided the ARP has been changed by the network.

**New Behavior**: New configuration commands available in this release

- First, create profiles for mapping ARP to RP values, and
- Second, associate the mapping with SGSN (3G) and GPRS (2G) services.

Using the ARP to RP mapping, the SGSN can choose a preferred radio priority according to the ARP values sent by the GGSN and HLR. As well, these mappings will be used by corresponding 2G and/or 3G services to choose the radio priority value while triggering messages (such as those listed below) towards the MS/UE:

- Activate PDP Accept.
- Modify PDP Request during network-initiated PDP modification procedure.
- Modify PDP Accept during MS-initiated PDP modification procedure provided the ARP has been changed by the network.

**Command Changes**

**qos-arp-rp-map-profile**

This new command, in the SGSN Global configuration mode, creates an ARP-RP mapping profile.

```
configure
  sgsn-global
    qos-arp-rp-map-profile  arp_profile_name
    no qos-arp-rp-map-profile  arp_profile_name
end
```
Notes:
- **arp_profile_name** - Enter a string of 1 to 64 alphanumeric characters to identify the mapping profile and moves into the ARP-RP mapping profile configuration mode.
- **no qos-arp-rp-map-profile** - Removes the profile definition from the configuration.

### Command Changes

**arp**

When the ARP-RP mapping profile is created, default ARP-RP mapping is automatically included (see default values in the Notes section below). This `arp` command, in the ARP-RP mapping profile configuration mode, modifies the ARP-RP mapping for the profile.

```plaintext
configure
  sgsn-global
    qos-arp-rp-map-profile arp_profile_name
      arp_value radio-priority rp_value
    end
```

Notes:
- **arp_value** - Defines the allocation retention priority. Enter an integer from 1 to 3.
- **rp_value** - Defines the radio priority. Enter an integer from 1 to 4.
- Default ARP-RP mapping would be
  - ARP1 RP4
  - ARP2 RP4
  - ARP3 RP4
- Use the `show sgsn-mode` command to display the ARP-RP profile and configuration.

### Command Changes

**sm radio-priority**

The `radio-priority` keyword is new in the `sm` commands in both the GPRS-Service and SGSN-Service configuration modes. This new keyword is used to associate an ARP-RP mapping profile with a 2G and/or a 3G service.

```plaintext
configure
  context context_name
    gprs-service service_name
      sm radio-priority from-arp arp_profile_name
      no sm radio-priority from-arp arp_profile_name
```

---

This document provides details on SGSN Changes in Release 15.0 and enhancements for October 31, 2014, outlining command changes related to ARP and radio priority configurations.
Notes:

- This example illustrates the GPRS Service configuration mode, but either GPRS or SGSN Service configuration modes could be entered. The command sequent would have to be repeated, once for each type of service, to associate the ARP-RP profile with both types of services.

- `no sm radio-priority from-arp` - This command will remove the association from the configuration.

- Use the `show configuration` command to display the association.

### CSCup94835 - SGSM/MME :PC: [0aae198f/X] client_bounce()

#### Feature Changes

**Avoiding SessMgr Broadcasts**

**Previous Behavior:** The IMSI-Mgr broadcasts to all SessMgrs when receiving an unknown IMSI request from the HLR.

**New Behavior:** New CLI disables the IMSI-Mgr from broadcasting (broadcasting is the default) to all SessMgrs when the IMSI-MGR finds a particular IMSI is unknown.

**Customer Impact:** The feature can be used ‘on the fly’ to reduce IMSI-Mgr high CPU usage if caused by huge numbers of broadcasts.

#### Command Changes

```bash
task facility imsimgr

A new keyword (`avoid-sessmgr-broadcast`) configures the SGSN’s IMSI-Mgr to avoid broadcast requests to session managers. By default, broadcasting is enabled. With this keyword, broadcasting can be disabled ‘on the fly’ if CPU usage is too high due to large number of broadcast messages.

configure

    task facility imsimgr avoid-sessmgr-broadcast

    [ no ] task facility imsimgr avoid-sessmgr-broadcast

end
```
SGSN Enhancements for June 6, 2014

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
- NAT Enhancements
- SNMP MIB Enhancements
- System and Platform Enhancements

---

**CSCuf25521 - show service all provides incorrect values**

**Feature Changes**

**Change in the Information Display**

**Previous Behavior:** Previously, the output generated by the *show service all* command displayed incorrect values for the Maximum Sessions field for both the GPRS Service (2G) and the SGSN Service (3G).

**New Behavior:** The output generated by the *show service all* command now displays correct values (which vary depending on the hardware) for the Maximum Sessions field for both the GPRS Service (2G) and the SGSN Service (3G).
CSCuj62285 - IP tcp mss settings on sgsn

Feature Changes

Making TCP MSS Configurable

**Previous Behavior:** The SGSN transparently passed the maximum segment size (MSS for TCP uplink/downlink traffic) in TCP SYN (and SYN-ACK) messages between UE and the server. In cases where the MSS value exchanged between UE and server is 1460 or more, with the addition of the GTP header, the packets often would be fragmented, which resulted in packets being dropped by network nodes that could not handle fragmentation.

**New Behavior:** To avoid fragmentation, the SGSN can now be configured to modify/overwrite the TCP MSS value exchanged between the UE and the server (for both 2G and 3G uplink/downlink traffic) if the requested value is more than the SGSN's locally configured value.

Command Changes

```
tcp-maximum-segment-size
```

This new command in the Call Control Profile configuration mode enables the operator to define a maximum segment size (MSS), that will be used to overwrite received TCP MSS values in uplink/downlink packets between UE to the server.

```
configure
call-control-profile profile_name
tcp-maximum-segment-size size
remove tcp-maximum-segment-size
end
```

Notes:
- `size` - is the maximum number of octets for a segment, value range is 1 to 1460.
- `remove` - as part of the command, returns the MSS to the SGSN’s default of 1460 octets.
- An additional Yes/No prompt is included due to the high impact of the MSS configuration.

CSCul70235 - 'show sgsn sessmgr all ptmsi statistics' displays NRI Values incorrectly

Feature Changes

Clarify Display Information
Previous Behavior: Previously, the `show sgsn sessmgr all ptmsi statistics` command included an `nri` parameter in the command that caused incorrect or confusing information to be displayed under the `NRI` heading in the output.

New Behavior: In the `show sgsn sessmgr all ptmsi statistics` command, the `nri` keyword option has been renamed as `ptmsi-pool-id`. As well, the NRI display heading in the output screen has also been renamed to `PTMSI pool ID`.

Customer Impact: Customer will need to use the new keyword when issuing the `show sessmgr all` command as the old keyword is no longer available.

CSCun89264, CSCuj65387 - [RIM] : Enhancements to Handling subsequent rim segments

Feature Changes

XUDTS Messages for RIM

Previous Behavior: The SGSN Link manager failed to handle segmented SCCP-XUDT messages resulting in segmented messages being dropped.

New Behavior: When the application layer message cannot be sent in a single SCCP-UDT message, then the SCCP layer segments the message into multiple XUDTS (Extended Unidata Service) messages and sends them over the network. The SGSN’s Link manager handles the XUDTS messages for RIM (RAN information request mechanism) by implementing segment handling and reassembly.

New counters have been added to peg handling of these segments (see Performance Indicator Changes below).

Performance Indicator Changes

show linkmgr

New counters have been added to the output of the `show linkmgr all parser statistics all` to peg LinkMGR handling of XUDTS message segments for RIM. The first is added in the Parser Statistics section and the second new counter is added to the Memory Cache Usage section of the output.

- The first 4 new counters are added in the Parser Statistics section of the output:
  - Segmented RIM tracks the number of RIM fragments received.
  - Out of Seq RIM tracks the out of sequence RIM fragments received.
  - Dup RIM tracks duplicate RIM entries and deletes them before creating a mapping entry in the LRN table.
  - Dup LRN tracks duplicate LRN entries and deletes them before creating a mapping entry in the RIM table.

- The last new counter is added to the Memcache Usage section of the output:
  - LRN RIM Entry tracks usage of memory cache blocks for RIM
CSCuo62754 - Assertion failure at sess/sgsn/sgsn-app/db/sgsn_db_pmm.c:1880

Feature Changes

Ready Timer During Attach/RAU

**Previous Behavior:** The Ready timer expiry is honored during ongoing Attach/RAU procedures.

**New Behavior:** The Ready timer expiry is not honored during ongoing Attach/RAU procedures.
SGSN Enhancements for April 10, 2014

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

---

CSCuj65387, CSCun89264 - [RIM] : Enhancements to Handling subsequent rim segments

**Feature Changes**

**XUDTS Messages for RIM**

**Previous Behavior:** The SGSN Link manager failed to handle segmented SCCP-XUDT messages resulting in segmented messages being dropped.

**New Behavior:** When the application layer message cannot be sent in a single SCCP-UDT message, then the SCCP layer segments the message into multiple XUDTS (Extended Unidata Service) messages and sends them over the network. The SGSN’s Link manager handles the XUDTS messages for RIM (RAN information request mechanism) by implementing segment handling and reassembly.

New counters have been added to peg handling of these segments (see *Performance Indicator Changes* below).
Performance Indicator Changes

show linkmgr

New counters have been added to the output of the `show linkmgr all parser statistics all` to peg LinkMGR handling of XUDTS message segments for RIM. The first is added in the Parser Statistics section and the second new counter is added to the Memory Cache Usage section of the output.

- The first 4 new counters are added in the Parser Statistics section of the output:
  - Segmented RIM  tracks the number of RIM fragments received.
  - Out of Seq RIM  tracks the out of sequence RIM fragments received.
  - Dup RIM        tracks duplicate RIM entries and deletes them before creating a mapping entry in the LRN table.
  - Dup LRN        tracks duplicate LRN entries and deletes them before creating a mapping entry in the RIM table.

- The last new counter is added to the Memcache Usage section of the output:
  - LRN RIM Entry  tracks usage of memory cache blocks for RIM
SGSN Enhancements for March 31, 2014

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

---

**CSCtz55422 - SGSN should start dns query for default SGSN when nri based query fails**

**Feature Changes**

**SGSN Support For RAI Based Query**

**Previous Behavior:** A DNS query with NRI is performed for ISRAU, Identification and Suspend Requests. Failure of the NRI based DNS query results in failure of the ISRAU, Identification and Suspend Requests. The SGSN does not support a RAI based query when NRI based query fails.

**New Behavior:** A new CLI option `rai-fqdn-fallback` is provided in the `peer-nri-length` CLI under the Call Control Profile Configuration, which allows the operator to configure the SGSN's support to fallback on RAI based query when NRI based query fails.
Command Changes

peer-nri-length

A new keyword `rai-fqdn-fallback` has been included in the `peer-nri-length` command, this keyword is configured to support RAI based query when NRI based query fails. This keyword is disabled by default.

```config
configure
call-control profile profile_name
  peer-nri-length length [rai-fqdn-fallback]
  remove peer-nri-length [rai-fqdn-fallback]
end
```

Notes:
- Currently, this feature is supported for 3G subscribers only.
- 2G Context Request and Identification Request messages are not supported.
- S4 support of this extensions for all applicable scenarios is not supported.

CSCuh86390 - [2G-MOCN]Counters for redirection complete sent in retry messages

Feature Changes

2G MOCN Counters Peg Retried Attach/RAU Accepts with Redirection Complete

**Previous Behavior:** SGSN has counters to peg the number of Attach/RAU Accept/Reject messages sent with redirection complete flag set.

**New Behavior:** New counters, with corresponding bulk statistics, peg the number of retried Attach/RAU Accepts with redirection complete at the stack level. Counters and stats are identified below in the Performance Indicator Changes section.

Performance Indicator Changes

SGSN Schema

New proprietary stats track, per RA level, the number of Attach Accepts or RAU Accepts the SGSN retransmits, with the redirection complete flag, when the SGSN has not received a response from the UE for transmitted messages Attach Accept or RAU Accept.

- 2g-attach-acc-retry-with-redir-comp
- 2g-rau-acc-retry-with-redir-comp

show gmm-sm statistics verbose
New display counters indicate the number of Attach/RAU Accepts retried with the redirection complete flag

- GPRS MOCN Attach Statistics
  - Attach Accept Retry with Redirection Complete
- GPRS MOCN RAU Statistics
  - RAU Accept Retry with Redirection Complete

**CSCuI55835 - qos-dscp no cs3 mode unavailable**

**Command Changes**

```bash
gtpc ip qos-dscp
```

The SGSN now supports selection of Class Selectors 0 through 7 in the configuration of QoS DSCP marking to be used when sending GTP-C messages. These eight new parameters are added to an existing list of options. Only the new parameters are noted below as selectable options:

```bash
configure

c_context context_name

  sgtp-service service_name

  gtpc ip qos-dscp { cs0 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 }

  default gtpc ip qos-dscp

end
```

**Notes:**

- `cs0 - cs7` identifies class selector modes 0 through 7 PHB
- `default` resets the DSCP marking configuration to the `be` (best effort forwarding) option.

**CSCuM03645 - LTE to 3G IRAT-idle mode failed due to missing RNC TEID in EGTP UBR.**

**Feature Changes**

**Avoiding S12 DT during Inter SGSN RAU**

**Previous Behavior:** Default behavior is to establish Direct Tunnel (DT) if it is permitted in SGSN’s Call-Control profile configuration.

**New Behavior:** The operator can modify the S4-SGSN’s Call-Control profile configuration to override the default behavior and configure the SGSN to avoid establishment of a Direct Tunnel, on the S12 interface, during RAU-based handovers.
Important: This new configuration functionality is not available for the Gn interface

Command Changes

rau-inter

A new CLI keyword `avoid-s12-direct-tunnel` enables the operator to modify the Call-Control profile default configuration and instructs the SGSN to avoid establishment of a Direct Tunnel for S12 interfaces.

```
configure

call-control-profile profile_name

rau-inter avoid-s12-direct-tunnel

[ default | remove ] rau-inter avoid-s12-direct-tunnel

end
```

Notes:

- Configuring this keyword will be ignored for Gn interfaces.
- `default` disables this new functionality and returns the profile’s configuration to the default functionality to automatically establish a direct tunnel when DT functionality is enabled in the Call-Control profile configuration.
- `remove` erases the S12 Direct Tunnel on Inter SGSN RAU line from the Call-Control profile configuration and returns the functionality to the default.

Performance Indicator Changes

show s4-sgsn statistics

A new counter has been added to indicate the number of PDPs setup during SGSN RAU that have not had direct tunnels established due to the ‘avoid’ configuration.

- 3G S4 PDPs with direct tunnel avoided during new SGSN RAU

CSCum52817 - Do Not establish RAB even if ASI bit is set

Feature Changes

Ignoring ASI bit when Establishing RAB during RAU-based Handover

Previous and Current Behavior: By default, the SGSN uses the ASI bit in SGSN Context Response to establish RAB during a RAU-based handover.

New Behavior: The operator can modify the SGSN service configuration to override the default behavior and configure the SGSN to ignore the ASI bit in the SGSN Context Response during RAU-based handovers, and to ignore establishing a RAB for any PDPs.
Important: The new CLI will not modify the default behavior for an S4 interface.

Customer Impact: Signaling reduction.

Command Changes

A new CLI keyword `ignore-asi` enables the operator to modify the SGSN service default configuration and instructs the SGSN to ignore the ASI bit in the SGSN Context Response during RAU-based handovers over Gn interfaces.

```
configure
  context context_name
    sgsn-service service_name
      sm ignore-asi
      no sm ignore-asi variable
    end
```

Notes:
- Configuring this keyword will be ignored for S4 interfaces.
- `no` disables this new functionality to ignore the ASI bit and returns the SGSN service configuration to use the ASI bit for RAB establishment.

Performance Indicator Changes

```
show sgsn-service name
```

A new field in the `show sgsn-service` output display indicates if the ‘ignore ASI’ functionality has been enabled.

- Ignore ASI bit received from peer SGSN during RAU : Enabled / Disabled

CSCum56947 - Configuration to enable sending extended MBR for UL/DL

Feature Changes

SGSN Support For Sending Extended Bits Bi-directionally

**Previous Behavior:** Support for sending extended bitrates in both uplink and downlink directions is absent.

**New Behavior:** Extended bitrates are included in both uplink and downlink direction when the negotiated bitrate indicates that extended bitrates should be included in one direction. A new CLI `ranap bidirectional-always ext-mbr-ie` is added under the RNC Configuration mode to enable sending extended bitrates bi-directionally.
Command Changes

**ranap bidirectional-always ext-mbr-ie**

This command enables or disables sending of extended bitrates bi-directionally. When this command is enabled, the specified extended bitrates (MBR or GBR) are included bi-directionally (uplink and downlink directions) in the RAB Assignment Request even if the negotiated bitrate indicates that extended bitrates should be included in one direction.

```plaintext
configure
context context_name
iups-service service_name
rnc id rnc_id

ranap bidirectional-always ext-mbr-ie [ext-gbr-ie]

no ranap bidirectional-always

end
```

Notes:

- When this command is configured, if the maximum bitrate for either uplink or downlink directions indicates that extended bitrates should be included (that is, the maximum bitrate negotiated value exceeds “16”Mbps in either uplink or downlink direction), then the maximum bitrate extended IE is included in both uplink and downlink directions. If in one direction (uplink or downlink) the negotiated value does not exceed “16” Mbps then extended maximum bitrate is sent as “16000001”.
- The keyword `ext-gbr-ie` is included to enable sending of Extended Guaranteed Bitrates IE.
- The `no` form of the command disables sending of both extended MBR and GBR bi-directionally.

**CSCum56967 - Security Issue - Encryption on MME/SGSN level**

Feature Changes

**Failure Action for Random IOV-UI Negotiation Failure**

**Previous Behavior:** The SGSN falls back to unencrypted mode whenever the XID negotiation for Random IOV-UI between the MS and the SGSN fails. This is irrespective of any ciphering algorithm configured.

In order to preserve the connection, the SGSN falls back to default encryption parameters whenever it fails to decipher an encrypted frame that is sent by the MS.

As a result of the above behavior, the MS users could be exposed to passive interception attacks, channel hijacking, or denial of service attacks.

**New Behavior:** In accordance with the 3GPP specification, once the encryption has been started, neither the MS nor the network shall go to an unciphered session. Thus, the SGSN’s default behavior to fallback to default IOV-UI is now changed to always reject the call.

In some situations of XID negotiation failure, the SGSN will respond as outlined in either CSCun09183 or CSCun13033.
Command Changes

```
llc random-value-in iov-ui
```

New configuration options, `negotiation-failure-action { fallback-to-default iovui | reject }`, enable the operator to specify the desired failure action to be performed whenever the random IOV-UI negotiation fails. The operator has the option to either:

- (a) reject the call whenever the deciphering fails due to the random IOV-UI negotiation failure (thus avoiding a security breach), or
- (b) to fall back to the default IOV-UI.

```
configure

c  ontext context_name

  gprs-service service_name

    llc random-value-in iov-ui [ negotiation-failure-action { fallback-to-default iovui | reject } ]

    default llc random-value-in iov-ui

end
```

Notes:

- `default` resets the SGSN configuration so that all calls are rejected whenever the deciphering fails due to failure of the XID negotiation for random IOV-UI.
- `reject` returns the SGSN to the default configuration to reject all calls when random IOV-UI negotiation fails.
- `fallback-to-default iovui` allows the operator to return to the previous behavior where the SGSN falls back to unencrypted mode whenever the XID negotiation for random IOV-UI negotiation fails.

Performance Indicator Changes

**show session disconnect-reasons verbose**

If configured for ‘Reject’, a new disconnect reason tracks the number of calls cleared due to the new default behavior to reject any call when random IOV-UI negotiation fails.

- `sgsn iovui-negotiation-failure(556)`

**show gprs-service name**

Configuration of this feature can be viewed in the output display of both the `show configuration` and the `show gprs-service` with a new display field.

- Random IOVUI negotiation failure action:
CSCum62465 - SGSN hangs and lots of Assertion failure at snutil/sn_memblock.c:188

Feature Changes

Handling of Retransmitted BSSGP Suspend Messages

**Previous Behavior:** Retransmitted BSSGP Suspend messages were handled when they were received.

**New Behavior:** Received retransmitted BSSGP Suspend messages are dropped and new statistic pegs duplicate inter-SGSN Suspend messages that are dropped.

Performance Indicator Changes

**show bssgp statistics**

The new counter, noted below, pegs the number of retransmitted BSSGP Suspend messages that are dropped:

- Inter-Sgn suspend message dropped

CSCum76067 - GMM-T3323 Timeout display some junk value under sgsn-service

Feature Changes

IDT and T3323-timeout Configuration Coordination

**Previous Behavior:** Configuration of GMM T3323-timeout in the SGSN service was allowed even if implicit-detach-timeout (IDT) under the `gmm` command in the SGSN service is not configured

**New Behavior:** SGSN behavior has been modified so that configuration of GMM T3323-timeout in the SGSN service is not allowed if implicit-detach-timeout under `gmm` in SGSN service is not configured.

**Customer Impact:** Adjustment for T3323 and IDT should be done properly, and if IDT is not configured, then configuration of T3323 is not permitted. If attempted the SGSN generates an error message.

CSCun09183 - SGSN should not cleanup the subscriber when XID exchange times out

Feature Changes

Subscriber Moves to STANDBY for XID Negotiation Failure

**Previous Behavior:** As a result of XID for random IOV-UI negotiation failure during intra-RAU or standalone authentication for SMS, the SGSN clears the subscriber.
New Behavior: Now, when XID for random IOV-UI negotiation failure occurs during intra-RAU or standalone authentication for SMS, the SGSN moves the subscriber to STANDBY and marks the XID negotiation as a failure. In some situations of XID negotiation failure, the SGSN will respond as outlined in CSCun13033.

CSCun13033 - Detach request is not triggered in following scenario

Feature Changes

Changes to handling of failures of XID negotiation for radome IOV-UI are also incorporated into related issues CSCum56967 and CSCun09183.

Responses to XID Negotiation Failure

Previous Behavior: SGSN clears the subscriber based on the configured negotiation failure action if the previous XID negotiation for random IOV-UI fails upon receiving any uplink packets whether ciphered or unciphered.

New Behavior: The SGSN manner of handling failure of XID negotiation for random IOV-UI has been modified, so that now the SGSN:

- Initiates XID for new random IOV-UI negotiation:
  1. with the MS is in STANDBY state, any uplink packet (in either ciphered or unciphered mode, except Attach / Intra-RAU) from the MS which results in CELL-UPDATE, READY TIMER START and RADIO STATUS READY causes an event indication to the application.

- Initiates Detach:
  1. with the MS is in STANDBY state, any uplink activity causes the SGSN to initiate a new XID exchange, which if it fails or aborts due to the reception of SUSPEND, RADIO-STATUS and READY-TIMER expiry, results in the SGSN initiating Detach.
  2. when PAGING is ongoing, any Page response from the MS results in the SGSN initiating Detach.
  3. during OLD_SGSN ISRAU, when any uplink data comes before T3 tunnel timer expiry then the SGSN initiates Detach.

- Handles Messages:
  1. Attach and intra-RAU (from both local and non-local TLLI or from both the same and different RA) will be processed in any state.

- Moves to STANDBY state:
  1. MS is moved to STAND-BY state if the XID exchange failed due to any of the following cases suspend, radio status, BVC block, BVC reset, ready timer expiry, no response received for XID exchange during INTRA-RAU/Standalone Authentication for SMS.
  2. XID is ongoing in READY state and if the MS moves to either 3G or to the peer-SGSN then the subscriber is moved to STANDBY state.

Also, all the uplink packets received from the MS (like ACTIVATE, ACTIVATE SECONDARY PDP, DE-ACTIVATE, MODIFY, SMS) will be dropped and the XID message will be retried whenever the XID is ongoing in READY STATE. Whenever the SGSN initiates the XID in READY state, it informs the GTP to stop forwarding the data if any is received for that MS. Upon the reception of XID response in READY state, GTP will be informed to start forwarding the data queued, if there is any.
SGSN Enhancements for January 31, 2014

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

### CSCue50555 - S-CDR should quantify the volume drop with probable cause code/counter

**Feature Changes**

**sgsn2gDlDroppedBytes**

The attribute `sgsn2gDlDroppedBytes` is added to 2G S-CDR in the custom33 dictionary (which requires a special license to use). This counter tracks the sum of the bytes dropped due to paging failure and the queue being full at the SGSN for 2G subscribers. This counter does not account for the data dropped due to any other causes.

This new S-CDR field is documented under CSCuJ86799 in the *GTPP Enhancements* section.
CSCui42601 - Require Intra-SRNS and Inter-SRNS bulkstat counter

Performance Indicator Changes

SGSN Schema

New bulk statistics have been added to correspond to Intra-SRNS and Intra-SRNS CLI counters output by the `show gmm-sm statistics` command:

<table>
<thead>
<tr>
<th>New Bulk Statistics</th>
<th>CLI Output Counter</th>
</tr>
</thead>
<tbody>
<tr>
<td>total_att_intra_sgsn_srns</td>
<td>3G-SRNS Stats / Attempted / Total SRNS:</td>
</tr>
<tr>
<td>att_intra_srsn_ue_involved</td>
<td>Intra-SGSN SRNS</td>
</tr>
<tr>
<td>att_intra_srsn_ue_not_involved</td>
<td>Intra-SRNS UE involved</td>
</tr>
<tr>
<td>total_att_inter_sgsn_srns</td>
<td>Intra-SRNS UE not involved</td>
</tr>
<tr>
<td>att_old_sgsn_inter_srsn_ue_involved</td>
<td>Inter-SRNS UE involved (old SGSN)</td>
</tr>
<tr>
<td>att_old_sgsn_inter_srsn_ue_not_involved</td>
<td>Inter-SRNS UE not involved (old SGSN)</td>
</tr>
<tr>
<td>att_new_sgsn_inter_srsn_ue_involved</td>
<td>Inter-SRNS UE involved (new SGSN)</td>
</tr>
<tr>
<td>att_new_sgsn_inter_srsn_ue_not_involved</td>
<td>Inter-SRNS UE not involved (new SGSN)</td>
</tr>
<tr>
<td>att_old_sgsn_inter_srsn_with_mme_ue_involved</td>
<td>Inter-SRNS UE involved (old SGSN with MME)</td>
</tr>
<tr>
<td>att_old_sgsn_inter_srsn_with_mme_ue_not_involved</td>
<td>Inter-SRNS UE not involved (old SGSN with MME)</td>
</tr>
<tr>
<td>att_new_sgsn_inter_srsn_with_mme_ue_involved</td>
<td>Inter-SRNS UE involved (new SGSN with MME)</td>
</tr>
<tr>
<td>att_new_sgsn_inter_srsn_with_mme_ue_not_involved</td>
<td>Inter-SRNS UE not involved (new SGSN with MME)</td>
</tr>
<tr>
<td>total_suc_intra_sgsn_srns</td>
<td>3G-SRNS Stats / Successful / Total SRNS:</td>
</tr>
<tr>
<td>suc_intra_srsn_ue_involved</td>
<td>Intra-SGSN SRNS</td>
</tr>
<tr>
<td>suc_intra_srsn_ue_not_involved</td>
<td>Intra-SRNS UE involved</td>
</tr>
<tr>
<td>total_suc_inter_sgsn_srns</td>
<td>Intra-SRNS UE not involved</td>
</tr>
<tr>
<td>suc_old_sgsn_inter_srsn_ue_involved</td>
<td>Inter-SGNS SRNS</td>
</tr>
<tr>
<td>suc_old_sgsn_inter_srsn_ue_not_involved</td>
<td>Inter-SGNS SRNS</td>
</tr>
<tr>
<td>suc_new_sgsn_inter_srsn_ue_involved</td>
<td>Inter-SGNS SRNS</td>
</tr>
<tr>
<td>suc_new_sgsn_inter_srsn_ue_not_involved</td>
<td>Inter-SGNS SRNS</td>
</tr>
<tr>
<td>suc_old_sgsn_inter_srsn_with_mme_ue_involved</td>
<td>Inter-SGNS SRNS</td>
</tr>
<tr>
<td>suc_old_sgsn_inter_srsn_with_mme_ue_not_involved</td>
<td>Inter-SGNS SRNS</td>
</tr>
<tr>
<td>suc_new_sgsn_inter_srsn_with_mme_ue_involved</td>
<td>Inter-SGNS SRNS</td>
</tr>
<tr>
<td>suc_new_sgsn_inter_srsn_with_mme_ue_not_involved</td>
<td>Inter-SGNS SRNS</td>
</tr>
</tbody>
</table>
CSCuj28230 - Additional specific 2G/3G counters for SGSN

Performance Indicator Changes

SGSN Schema

22 bulk statistics for Attach Reject have been added to co-relate with the counters displayed through `show gmm statistics verbose`:

<table>
<thead>
<tr>
<th>New Bulk Stat</th>
<th>CLI Output Counter</th>
</tr>
</thead>
<tbody>
<tr>
<td>2G Attach Reject due to network failures (PS-Only Attach procedure)</td>
<td></td>
</tr>
<tr>
<td>2G-attach-rej-network-failure-no-data-from-hlr</td>
<td>2G-Data missing from HLR</td>
</tr>
<tr>
<td>2G-attach-rej-network-failure-congestion-thrtl</td>
<td>2G-Throttling due to Congest</td>
</tr>
<tr>
<td>2G-attach-rej-network-failure-check-imei-timeout-eir</td>
<td>2G-Check IMEI timeout EIR</td>
</tr>
<tr>
<td>3G Attach Reject due to network failures (PS-Only Attach procedure)</td>
<td></td>
</tr>
<tr>
<td>3G-attach-rej-network-failure-no-data-from-hlr</td>
<td>3G-Data missing from HLR</td>
</tr>
<tr>
<td>3G-attach-rej-network-failure-congestion-thrtl</td>
<td>3G-Throttling due to congest</td>
</tr>
<tr>
<td>3G-attach-rej-network-failure-opr-policy-failure</td>
<td>3G-Operator Policy Failure</td>
</tr>
<tr>
<td>3G-attach-rej-network-failure-check-imei-timeout-eir</td>
<td>3G-Check IMEI timeout EIR</td>
</tr>
<tr>
<td>3G-attach-rej-network-failure-rnc-ovld</td>
<td>3G-RNC Overload</td>
</tr>
<tr>
<td>3G-attach-rej-network-failure-more-ius-same-imsi</td>
<td>3G-Too many IUs same IMSI</td>
</tr>
<tr>
<td>3G-attach-rej-network-failure-no-resource-intl-failure</td>
<td>3G-Session mngr no resource</td>
</tr>
<tr>
<td>2G Attach Reject due to network failures (Combined Attach procedure)</td>
<td></td>
</tr>
<tr>
<td>2G-comb-attach-rej-network-failure-no-data-from-hlr</td>
<td>2G-Data missing from HLR</td>
</tr>
<tr>
<td>2G-comb-attach-rej-network-failure-congestion-thrtl</td>
<td>2G-Throttling due to Congest</td>
</tr>
<tr>
<td>2G-comb-attach-rej-network-failure-check-imei-timeout-eir</td>
<td>2G-Check IMEI timeout EIR</td>
</tr>
<tr>
<td>3G Attach Reject due to network failures (Combined Attach procedure)</td>
<td></td>
</tr>
<tr>
<td>3G-comb-attach-rej-network-failure-no-data-from-hlr</td>
<td>3G-Data missing from HLR</td>
</tr>
<tr>
<td>3G-comb-attach-rej-network-failure-congestion-thrtl</td>
<td>3G-Throttling due to congest</td>
</tr>
</tbody>
</table>
New Bulk Stat | CLI Output Counter
---|---
3G-comb-attach-rej-network-failure-check-imei-timeout-eir | 3G-Check IMEI timeout EIR
3G-comb-attach-rej-network-failure-rnc-ovld | 3G-RNC Overload
3G-comb-attach-rej-network-failure-more-ius-same-imsi | 3G-Too many Ius same IMSI
3G-comb-attach-rej-network-failure-no-resource-intl-failure | 3G-Session mngr no resource

CSCuj73484 - GPRS MOCN: Bulkstats to be added for counters

Performance Indicator Changes

SGSN Schema

The 28 new bulk statistics listed below have been added to enable the SGSN to track 2G MOCN-related parameters sent with Attach or RAU Requests, Accepts, and Rejects:

- 2g-total-attach-redir-attempt
- 2g-attach-req-redir-attempt-with-imsi
- 2g-attach-req-redir-attempt-without-imsi
- 2g-total-attach-redir-comp
- 2g-attach-redir-comp-success
- 2g-attach-redir-comp-failure
- 2g-attach-redir-indication
- 2g-attach-redir-ind-ill-plmn
- 2g-attach-redir-ind-ill-la
- 2g-attach-redir-ind-no-roam
- 2g-attach-redir-ind-no-gprs-plmn
- 2g-attach-redir-ind-no-cell-in-la
- 2g-attach-redir-ind-csp-req
- 2g-attach-redir-ind-others
- 2g-total-rau-redir-attempt
- 2g-rau-req-redir-attempt-with-imsi
- 2g-rau-req-redir-attempt-without-imsi
- 2g-total-rau-redir-comp
- 2g-rau-redir-comp-success
- 2g-rau-redir-comp-failure
- 2g-rau-redir-indication
CSCuj73688 - EMS support required for new counters in SGSN gmm-sm
Statistics

Feature Changes

WEM Support for New Bulk Statistics

WEM support has been added for the 28 new SGSN Schema statistics identified in CSCuj73484.
SGSN Enhancements for November 30, 2013

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 & Platform Enhancements

---

**CSCua59413 - SGSN support required to route Direct InformationTransfer msg to eNB**

**Feature Changes**

**RIM Msg Transfer to MME via GTPv1**

RAN Information Management (RIM) procedures provide a mechanism for the exchange of information between RAN nodes. This information is transferred in RIM containers via messages which are routed and relayed independently via the SGSNs.

Previously, the SGSN supported RIM messages from BSS/RNC to another BSS/RNC belonging to a different or the same SGSN over GTPv1 protocol. Now, the SGSN also supports transfer of RIM messages to/from an MME (eNodeB) via GTPv1 protocol.
The SGSN uses existing CLI to enable the RIM transfer functionality. Whether or not the RIM message goes from/to BSC/RNC to/from BSC/RNC or to/from eNodeB is determined by the addressing. To transfer RIM messages to the MME (eNodeB),

- requires RIM functionality be enabled for the SGSN.
- requires the DNS server be configured to respond to a TAI-based DNS query in the following format

\[
tac-lb<TAC-low-byte>.tac-hb<TAC-high-byte>.tac.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org
\]

OR

- requires the MME (eNodeB) address be added to the SGSN’s Call Control Profile

For more information about RIM on the SGSN and configuration details, refer to the RIM Message Transfer feature chapter in the SGSN Administration Guide.

**CSCue89610 - [15.0] Route to remote PC via linkset not removed on deletion of linkset**

**Feature Changes**

**Linkset Route Optimization**

This change is a part of the route optimization process started with 15.0 FCS.

**Previous Behavior:** As a part of the route optimization process, all peer-server (PS) routes were deleted when the PS configuration was deleted from the proprietary SS7 routing domain configuration. There was not a mirror mechanism for linkset routes.

**New Behavior:** As a part of the route optimization process, all linkset (LS) routes are deleted when the linkset configuration is deleted from the proprietary SS7 routing domain configuration. This mirrors the mechanism for PS routes. This change is reflected by the link manager.

**Customer Impact:** It will impact service if the linkset configuration is deleted from the SS7RD.

**CSCuh34654 - IDT in 2g should be supported for both Gn and S4 SGSN**

**Feature Changes**

**Timer Display Controlled by ISR License**

**Previous Behavior:** T3323 Timer in the SGSN Service and the GPRS service and IDT timers in the GPRS Service were displayed even if the ISR license was not installed.

**New Behavior:** T3323 Timer in the SGSN Service and the GPRS service and IDT timers in the GPRS Service are displayed only if the ISR (Idle Mode Signaling Reduction) license is installed.
CSCuh99198 - CLI config to Accept RAB negotiation for PDP Activation in S4-SGSN

Feature Changes

Configurable Control of RAB Negotiation in S4-SGSN

Previous Behavior: Per TS 23.060 section 9.2.2.1A, the S4-SGSN rejects PDP activation if RNC negotiates QoS during RAB assignment.

However, in some networks, the RNCs do negotiate QoS due to:

1. RNC is pre-R9 and the network knows that the UE is not capable beyond certain bit rates. So it negotiates the MBR / GBR values to what is acceptable to the UE.
2. RNC has resource constraints or it is a legacy RNC capable of only certain bit rates, hence the network gives only what is possible for the RNC to accept.

Scenario 1 is the most common case in a Gn SGSN + pre-R9 RNC deployment. But case (1) means the UE is not EPC-capable so the SGSN will not allow use of the S4 interface for such UEs -- unless the UE has an EPS subscription.

Scenario 2, the S4-SGSN rejects PDP activation.

New Behavior: To allow customers to support legacy RNCs, the SGSN now supports a new CLI to configure S4-SGSN acceptance of PDP activation even with such legacy RNCs. The CLI changes are documented below and use requires the S4-SGSN license.

Customer Impact: Provides flexibility to control S4-SGSN behavior based on CLI configuration if RNC negotiates QoS. A CLI modification is needed for activation case alone as the default behavior, per 3GPP spec, is to reject activation, which is service impacting. Hence, to avoid such service impacts a configuration is added to control the behavior.

Command Changes

qos-modification

If the S4 interface is used for PDP activation and the new keyword allow-s4-rab-negotiation is configured, then the SGSN locally accepts what the RNC sends as QoS in the RAB Assignment Response and sends that QoS in the Activate Accept.

configure

    context context_name

    sgsn-service sgsn_service_name

    qos-modification { inform-rnc-before-ue | allow-s4-rab-negotiation }

[ no ] qos-modification [ inform-rnc-before-ue | allow-s4-rab-negotiation ]

end

Notes:

- The SGW and/or PGW will not be informed of the modified QoS, which is a per bearer MBR / GBR rate.
- New keyword will only be applicable during PDP activation and not during intra RAU / SRNS / HSS init modification,

**Performance Indicator Changes**

**show sgsn-service**

A new field with either ‘Allowed’ or ‘Not Allowed’ options has been added to the output of the `show sgsn-service service_name` to indicate whether or not this new functionality has been configured:

- RNC QoS Negotiation for S4-SGSN:
- 3G S4 PDP Activation Rejects due to RAB Negotiation

**show s4-sgsn statistics**

New counters track the PDP activation statistics related to RAB negotiations:

- 3G S4 PDPs with RAB Negotiation Locally Accepted
- 3G S4 PDP Activation Rejects due to RAB Negotiation

**CSCui65204 - [EDR]: SNMP trap not generating after EDR file deletion**

**Feature Changes**

**Configuring for SNMP Trap Messages**

**Previous Behavior:** When the EDR record files are purged no SNMP trap messages are sent.

**New Behavior:** When the EDR record files are purged, SNMP trap messages will be sent for each file purged if existing "trap-on-file-delete" option is configured.

```plaintext
configure

context context_name

  session-event-module

    file trap-on-file-delete

end
```

**CSCuj13922 - Text string is not displayed properly in GMM INFO msg in this scenario**

**Feature Changes**

**Network Name in GMM Info Msg**
**Previous Behavior:** In the BSSAP message, printing full network name and short name was displayed as Hex values for all coding scheme values (0, 1, and 2).

**New Behavior:** When using the Monitor Protocol utility to view BSSAP messages sent by SGSN at Attach, only coding scheme values 0 and 1 are supported and the network name will be printed as the full name rather than as a Hex value.
SGSN Enhancements for September 30, 2013

SGSN Feature Changes as of September 30, 2013

This section provides information on SGSN feature changes in release 15.0.

**Important:** For more information regarding features in this section, refer to the *Cisco ASR 5000 Serving GPRS Support Node Administration Guide* for this release.

New SGSN Features

This section identifies new SGSN features available in release 15.0.

**Important:** Note that the S4 functionality and Location Services functionality noted below are qualified for Lab and Field Trial deployments only.

Lawful Intercept Support for 3G Direct Tunnel

Previously, when a warrant was placed on the SGSN via the Lawful Intercept (LI) system for a specific 3G subscriber, the subscriber was taken out of the direct-tunnel mode and returned back to 2-tunnel mode. The 3G Direct Tunnel enhancement for LI now provides for the ability to continue in the 3G direct-tunnel mode. For more information on Lawful Intercept, contact your Cisco representative.

AAA Changes To Support Location Services (LCS) Feature

The Location Services (LCS) feature in SGSN provides the mechanism to support mobile location services for operators, subscribers and third party service providers. AAA changes have been made to support the LCS feature. A new CDR type Mobile Originated Location Request CDRs (LCS-MO-CDR) is introduced. LCS-MO-CDRs support the standard dictionaries.

For detailed information on LCS-MO-CDRs, refer to the *Cisco ASR 5x00 GTPP Interface Administration and Reference*.

BSSGP Stack IEs Needed for 2G MOCN

The following IEs are added to DL-UNITDATA BSSGP message or to UL-UNITFATA BSSGP message in support of the new 2G MOCN functionality. To enable use of these IEs, MOCN must be enabled with the `gprs-mocn` command in the SGSN-Global configuration mode.

- DL-UNITDATA message:
  - Redirection-Indication
  - Redirection-Completed
  - Unconfirmed Send State variable
  - Initial LLC-PDU
• UL-UNITDATA message:
  • Redirect Attempt Flag
  • IMSI
  • Unconfirmed Send State variable

**Direct Tunnel Support on S4-SGSN**

Direct tunnelling of user plane data between the RNC and the S-GW can be employed to scale UMTS system architecture to support higher traffic rates. The direct tunnel (DT) approach optimizes core architecture without impact to UEs and can be deployed independently of the LTE/SAE architecture.

SGSN always supported DT in the 3G Gn/Gp SGSN and now DT support is added to the S4-SGSN to enable the establishment of a direct tunnel over the S12 interface between an RNC and an S-GW in a PS domain under a range of scenarios, such as (but not limited to):

- Primary PDP activation
- Secondary PDP activation
- Service Request Procedure
- Intra SGSN Routing Area Update without SGW change
- Intra SGSN Routing Area Update with SGW change
- Intra SGSN SRNS relocation without SGW change
- Intra SGSN SRNS relocation with SGW change
- Network-Initiated PDP Activation

The following scenarios (and others) exhibit procedural differences when an S4-SGSN DT is established:

- RAB Release
- Iu Release
- Error Indication from RNC

For a complete list of scenarios and a fuller description of this feature and its configuration requirements, refer to the *S4-SGSN Direct Tunnel Solution* chapter in the *Serving GPRS Support Node Administration Guide*

**EDR Enhancements**

A new event-logging handle has been introduced. In earlier releases the EDR module was used for event logging purpose, from this release onwards CDR_MODULE_EVENT_RECORD is used instead of CDR_MODULE_EDR. In Release 12.0, for generating event logs the SGSN re-used the existing “EDR” module which is primarily used for charging records. But from Release 15.0 onwards, the session-event module will be used by SGSN for event logging.

The CLI options present under the EDR Module are also present under the Session Event Module.

**Enhancement to S4-SGSN Statistics**

A new counter has been added to the output of the `show s4-sgsn statistics` command. This counter increments when a PDP is removed upon receiving a Delete Bearer Request (DBR) from a New SGW during Intra-SRNS relocation. This scenario can occur if the DBR is initiated from a New SGW before a Modify is received at its end.

**Expanded LCS Support**
With Release 14.0 SGSN supported basic Location Services (LCS) functionality. Now, with Release 15.0, supported functionality has expanded to include:

- Mobile terminating deferred location requests are now supported
- Mobile originating requests are now supported, both immediate and deferred
- Differences between 2G and 3G LCS call flows are eliminated

**Flex Pooling (lu / Gb over S16) Support on the S4-SGSN**

This feature adds the SGSN Pooling functionality across S16 (peer S4-SGSN) interface, so that the default SGSN can forward the received Context Requests from the non-Pooled SGSN to the right pooled SGSN, based on the NRI in P-TMSI. Flex pooling provides better scalability and load balancing. A new CLI command for pooling has been provided under eGTP Service Configuration to enable S4-SGSN pooling across the S16 interface. For more information on the command, refer to the *Cisco ASR 5x00 Command Line Interface Reference Manual*.

This feature requires the SGSN S3/S4 license and Flex feature license - no additional feature licenses are required.

**GPRS Multi-Operator Core Network**

In a Multi-Operator Core Network (MOCN), the radio network is shared among different operators, while each operator maintains its separate core network. The SGSN now supports MOCN in 2G, as well as 3G scenarios.

Sharing of radio resources and network nodes requires a PLMN network to support more than one PLMN-Id. A Public Land Mobile Network (PLMN) is uniquely identified by the combination of a mobile country code and a mobile network code (the PLMN-Id).

For a complete description of this feature and its configuration requirements, refer to the 2G SGSN Multi-Operator Core Network chapter in the *Serving GPRS Support Node Administration Guide*.

---

**Important:** The network sharing functionality now requires a feature license covering both 2G and 3G scenarios. Contact your Cisco representative for licensing details.

**Inclusion of IMSI in MAP-MO-FORWARD-SHORT-MESSAGE**

In accordance with 3GPP specification 29.002 V6 section 12.2, the SGSN can now be configured to include the IMSI of the originating subscriber in the mobile-originated SM transfer. This parameter shall be included when the sending entity (MSC or SGSN) supports mobile number portability (MNP). This IMSI IE is required in the in MAP-MO-FORWARD-SHORT-MESSAGE in countries where MNP is deployed.

**ISR with Circuit Switched Fallback (CSFB)**

**Circuit-Switched Fallback (CSFB)** is an alternative solution to using IMS and SRVCC to provide voice services to users of LTE. The IMS is not part of the solution, and voice calls are never served over LTE. Instead, the CSFB relies on a temporary inter-system that switches between LTE and a system where circuit-switched voice calls can be served.

The LTE terminals ‘register’ in the circuit switched domain when powered and attaching to LTE. This is handled through an interaction between the MME and the MSC-Server in the circuit-switched network domain over the SGs interface.

Consider the following scenarios:

- Voice calls initiated by the mobile user: If the user makes a voice call, the terminal switches from a LTE system to a system with circuit-switched voice support. Depending on where the UE latches on after completion of the voice call:
• The packet-based services that are active on the end-user device at this time are handed over and continue to run in a system with circuit-switched voice support but with lower data speeds.

OR

• The packet-based services that are active on the end-user device at this time are suspended until the voice call is terminated and the terminal switches back to LTE again and the packet services are resumed.

• Voice calls received by the mobile user: If there is an incoming voice call to an end-user that is currently attached to the LTE system, the MSC-Server requests a paging in the LTE system for the specific user. This is done through the SGs interface between the MSC Server and the MME. The terminal receives the page, and temporarily switches from the LTE system to the system with circuit-switched voice support, where the voice call is received. Once the voice call is terminated, the terminal switches back to the LTE system.

For detailed feature description see, Cisco ASR 5000 Serving GPRS Support Node Administration Guide.

ISR Support for GPRS

With release 14.0, Idle Mode Signaling Reduction (ISR) support was introduced for UMTS network access. With release 15.0, ISR support is now available for GPRS network access.

The ISR feature on the S4-SGSN provides a mechanism to optimize and/or reduce signaling load during inter-RAT cell-reselection in idle mode (that is, in the ECM-IDLE, PMM-IDLE, and GPRS-STANDBY states). It is a mechanism that allows the UE to remain simultaneously registered in a UTRAN/GERAN Routing Area (RA) and an E-UTRAN Tracking Area (TA) list. This allows the UE to make cell reselections between E-UTRAN and UTRAN/GERAN without having to send any TAU or RAU requests, as long as the UE remains within the registered RA and TA list.

ISR is a feature that reduces the mobility signalling and improves the battery life of UEs. ISR also reduces the unnecessary signalling with the core network nodes and air interface. This is important especially in initial deployments when E-UTRAN coverage will be limited and inter-RAT changes will be frequent.

The benefit of the ISR functionality comes at the cost of more complex paging procedures for UEs, which must be paged on both the registered RA and all registered TAs. The HSS also must maintain two PS registrations (one from the MME and another from the SGSN).

Important: The Gn/Gp SGSN does not support ISR functionality.

Important: The ISR feature requires a separate feature license. Contact your Cisco representative for licensing information.

NAPTR-based Dynamic HSS Discovery

In releases prior to R15.0, the SGSN could contact a HSS only through static configuration of the HSS peer end point through the HSS service. From Release R15.0 onwards, dynamic peer discovery is supported. The HSS address will be resolved using NAPTR based DNS request-response method. The following commands have to be enabled for dynamic peer discovery:

• In the Context Configuration Mode, the command `diameter endpoint < endpoint_name >` has to be enabled.

• In the Diameter Endpoint Configuration Mode, the command `dynamic-peer-discovery [ protocol { sctp | tcp } ]` has to be enabled.

• In the Diameter Endpoint Configuration Mode, the command `dynamic-peer-realm < realm_name >` has to be enabled.
• In the Diameter Endpoint Configuration Mode, the command `dynamic-peer-failure-retry-count <no_of_retries>` has to be enabled.

The “realm name” is used for dynamic peer discovery. The “dynamic-peer-failure-retry-count” is used to configure the number of re-tries in peer discovery.

**NRSPCA Support for S4-SGSN**

The SGSN supports Secondary PDP context activation by the network. 3GPP TS 23.060 specifies two procedures for GGSN-initiated PDP Context Activation:

• Network Requested PDP Context Activation (NRPCA) - the SGSN already supports this but only for 3G access, and

• Network Requested Secondary PDP Context Activation (NRSPCA) Procedure.

NRSPCA allows the network to initiate Secondary PDP context activation if the network determines that the service requested by the user requires activation of an additional secondary PDP context. Network requested bearer control makes use of the NRSPCA procedure.

Network requested bearer control functionality is mandatory in EPC networks, requiring use of NRSPCA. The P-GW supports only the NRSPCA procedure. With this release, now the S4-SGSN supports network requested bearer control.

For a complete description of this feature and its configuration requirements, refer to the *Network Requested Secondary PDP Context Activation* chapter in the *Serving GPRS Support Node Administration Guide*.

---

**Recovery Support for Stored BCM Mode**

**Previous Behavior:** SGSN did not display information for received BCM mode received from the GGSN.

**New Behavior:** SGSN now displays information for received BCM mode received from the GGSN for each PDP context.

**S4-SGSN Support for Fallback to V1 Cause Code in GTPv2 Context Response**

As per revised 3GPP TS 29.274 v8.6.0, the Context Response message received from a peer SGSN can have a cause code “Fallback to GTP-V1”, if the peer SGSN had provided a Gn interface for a subscriber due to local policy. When a new SGSN receives a Context Response with cause code as “Fallback to GTP-v1” it performs a GTP-v1 SGSN Context Request, Context Response and Context Ack with the peer SGSN to obtain the subscribers MM and PDP contexts.

**S4-SGSN Suspend-Resume Feature**

The S4-SGSN Suspend/Resume feature provides support for suspend/resume procedures from the BSS and a peer S4-SGSN. Suspend/resume procedure support was already supported for 3G services on the Gn/Gp SGSN.

When a UE is in a 2G coverage area wants to make a circuit switched voice call but the Class A mode of operation is not supported by the network, then the packet switched data session (PDP contexts) must be suspended before the voice call can be made. In this case, the BSS sends a Suspend Request to the SGSN. If the UE is already attached at that SGSN then the suspend request is handled via an intra-SGSN suspend/resume procedure. If the UE is not attached at the SGSN then the Suspend Request is forwarded to a peer SGSN/MME through GTPv2 and an inter-SGSN/SGSN-MME suspend procedure occurs. Once the UE completes the voice call, either the BSS sends a resume request to resume the
suspended PDPs or the UE directly sends a Routing Area Update Request (RAU) in 2G which will be treated as an implicit resume.

The ability for a GPRS user to access circuit-switched services depends on the subscription held, the network capabilities, and the MS capabilities.

For more information on this feature, refer to the S4-SGSN Suspend-Resume Feature chapter in the ASR 5000 SGSN Administration Guide.

Support for Supplementary Services

As part of the Location Services (LCS) enhancements, support has been implement for Supplementary Service procedures as provided in 3GPP TS 24.030, including:

- LCS Location Notification Invoke
- LCS Location Notification Return Result
- LCS Area Event Invoke
- LCS Area Event Invoke Ack
- LCS Area Event Report
- LCS Area Event Cancel
- LCS Area Event Cancel Ack
- LCS Periodic Location Invoke
- LCS Periodic Location Invoke Ack
- LCS Location Update
- LCS Location Update Ack
- LCS Periodic Location Cancel
- LCS Periodic Location Cancel Ack
- LCS MO-LR Invoke
- LCS MO-LR Return Result

Synchronization of Crash Events and Minicores Between Management Cards

The crashlog is unique to each of the management cards, so if a crash occurs when card the “8” is active it will be logged on card “8”. A subsequent switchover would no longer display the crash in the log. To retrieve this crash, a switch back over to card “8” has to be done. The crash event log and dumps are unique to active and standby management cards, so if a crash occurs on an active card then the crash event log and related dumps will be stored on an active card only. This crash information is not available on the standby card. Whenever the cards switchover due to a crash in the active card, and crash information is no longer displayed on the card which takes over. Crash information can be retrieved only from the current active card. To retrieve the crash list of the other card a switchover is required again. To avoid this switchover and to obtain the crash information from the standby card, synchronization between two management cards and maintaining latest crash information is required.

The arriving crash event will be sent over to the standby SMC/MMIO and saved in the standby’s crashlog file in the similar manner. Minicore, NPU or kernel dumps on flash of active SMC/MMIO needs to be synchronized to standby SMC/MMIO using the ‘rsync’ command. When a crashlog entry or the whole list is deleted through the CLI command, it should be erased on both active and standby SMCs/MMIOs. There is no impact on memory. All the crash related
synchronization activity will be done by the evlogd of standby SMC/MIO card, as the standby evlogd is less loaded and the standby card has enough room for synchronization activity. Therefore the performance of the system will not be affected.

**Zero Volume S-CDR Suppression**

This feature is developed to suppress the CDRs with zero byte data count, so that the OCG node is not overloaded with a flood of CDRs. The CDRs can be categorized as follows:

- **Final-cdrs:** These CDRs are generated at the end of a context.
- **Internal-trigger-cdrs:** These CDRs are generated due to internal triggers such as volume limit, time limit, tariff change or user generated interims through the CLI commands.
- **External-trigger-cdrs:** These CDRs are generated due to external triggers such as QoS Change, RAT change and so on. All triggers which are not considered as final-cdrs or internal-trigger-cdrs are considered as external-trigger-cdrs.

The customers can select the CDRs they want to suppress. This feature is disabled by default to ensure backward compatibility.

**Modified SGSN Features**

This section identifies SGSN features modified in release 15.0.

---

**Important:** Note that the S4 functionality and Location Services functionality noted below are qualified for Lab and Field Trial deployments only.

---

**Basic Location Service (LCS) Support**

With Release 14.0 SGSN initial support was provided for basic Location Services (LCS) functionality to collect and use or share location (geographical position) information for connected UEs in support of a variety of location services, such as location-based charging and positioning services. The SGSN uses the Lg interface to the gateway mobile location center (GMLC), which provides the mechanisms to support specialized mobile location services for operators, subscribers, and third party service providers.

Use of the Location Services (LCS) feature and the Lg interface is license controlled.

Basic LCS is now fully qualified. With this release, the functionality has been expanded - refer to R7 Location Services (LCS) - Phase 2.

The basic feature and configuration were described in the Location Services chapter in the Serving GPRS Support Node Administration Guide. The commands listed in the configuration chapter (new in Release 14.0) are available in the Command Line Interface Reference.

**Checksum Enabled With or Without Optimization**

The S4-SGSN now supports use of `no-optimize` keyword to enable/disable optimization for UDP checksum (refer to the Command Line Interface Reference for information about the `udp-checksum` command in the GTPU Service configuration mode).

**Previous Behavior:** By default, when UDP checksum was enabled, no optimization was attempted.

**New Behavior:** By default, the S4-SGSN now attempts optimization of UDP checksum in the UDP header of the GTPU packet. As well, it is now possible for optimization to be enabled or disabled as the S4-SGSN now supports use of the `no-optimize` keyword.
Configurable Pacing of PDP Deactivations on the S4-SGSN

The S4-SGSN now supports configurable pacing of PDP deactivations towards UEs due to path failures. Previously in the S4-SGSN, the pacing of path failure delivery was started by the EGTP application and it used the generic session manager pacing mechanism. The generic pacing mechanism performed 1000 path failure initiated PDP deactivations per second per session manager. Since this may not be desirable for many operators based on their RAN's capability, the S4-SGSN now supports the configurable pacing of PDP deactivations via the SGSN application (the same mechanism used in the Gn/Gp SGSN).

The existing **pdp-activation-rate command** in **SGSN Global Configuration Mode** can be used to configure the pacing of PDP deactivations for both the connected-ready state and the idle-standby state.

This feature is included with the SGSN S3/S4 license. No additional feature license is required.

**Previous Behavior:** On the S4-SGSN, when an SGW path failure occurs, all the PDPs anchored through that SGW will be deactivated at the rate of 1000 deactivations per second per session manager. This deactivation rate puts significant load on the RAN.

**New Behavior:** The existing **pdp-activation-rate command** in **SGSN Global Configuration Mode** can be used to configure the pacing of PDP deactivations for both the connected-ready state and the idle-standby state on the S4-SGSN.

Correct Context Object Names For Trap Numbers

**Previous Behavior:** The old system is declared with wrong context object names for the trap numbers 1180,1181,1183,1184,1185,1186, and 1187 in “starent.my” file.

**New Behavior:** The new system has correct context object names in “starent.my” file for the trap numbers 1180,1181,1183,1184,1185,1186, and 1187.

**Impact:** The customer can now see correct context object names in “starent.my” file for the trap numbers 1180,1181,1183,1184,1185,1186, and 1187.

Counters of RAB Release Messages Modified

**Previous Behavior:** If the RAB assignment request contains a RAB release list with multiple RAB Ids, then the RAB Release Attempted count was incremented by the number of RAB Ids contained within the RAB assignment request.

Similarly, if the RAB assignment response carries a RAB release list with multiple RAB Ids, then RAB Release Accepted count was incremented by the number of RAB Ids contained within the RAB assignment response.

**New Behavior:** If the RAB assignment request contains a RAB release list with single or multiple RAB Ids then, the RAB Release Attempted count is incremented by one count.

Similarly, if the RAB assignment response carries RAB release list with single or multiple RAB Ids then, the RAB Release Accepted count is incremented by one count.

Counters to Track Invalid IMSI Detach Requests

**Previous Behavior:** If an imsi-detach-request is received before security is complete for Activation/SMS, no counters are available to count such invalid imsi-detach-requests.

**New Behavior:** New counters are added to the show command **show gmm-sm statistics** to count invalid imsi-detach-requests.

CS-PS Coordination Check for 3G Network Sharing
Previous Behavior: Support available only to enable/disable cs-ps coordination check if 3G network-sharing was enabled in the IuPS service configuration mode.

New Behavior: Selective differentiation now configurable for homer and roamer for 3G network-sharing in the IuPS service configuration mode.

Deferred LCS Requests - Supplementary Service Messages

Previous Behavior: No supplementary service messages support for deferred LCS Requests.

New Behavior: New supplementary service messages are implemented to support deferred LCS Requests.

Detailed Failure Counters for MAP

Previous Behavior: Counters were not included.

New Behavior: As part of the enhanced LCS functionality in this release, new counters have been added to indicate different failure responses for MAP Provide Subscriber Location responses.

Diameter to GMM Cause Code Mapping For Diameter Error Code 5001 Changed

Previous Behavior: The diameter error code 5001 was mapped to GMM cause code “7” (GPRS services not allowed).

New Behavior: GMM cause code 8 will be sent as part of reject message when diameter error code “5001” is received. This change is observed by enabling the GMM protocol under monitor-protocol.

DPC Limit Enhancement for Loadsharing

Some customers required more than the allowed maximum number of DPCs that the SGSN supported for load sharing for an IMSI range. As a result, the software has been enhanced to increase the allowed maximum number of DPCs supported for load sharing for an IMSI range.

Previous Behavior: The maximum number of destination point codes (DPCs) the SGSN supported for load-sharing for an IMSI range was limited to 5.

New Behavior: In this release, the DPC limit has been increased to 20 per IMSI range.

Enhancing Link Management Mechanisms

Due to enhancements in hardware, processors, and management mechanisms for the ASR 5000, there has been an increase in the number of subscribers supported. The entry point for all signaling packets into the SGSN is the link management mechanism known as the LinkMgrs, which handle SIGTRAN, broadband, and narrowband traffic. To avoid LinkMgr overload and congestion, and waste of capacity, the number of LinkMgr instances has been modified.

Previous Behavior: Maximum number of instances of LinkMgrs has been 4, with 4 as the default.

New Behavior: Maximum number of instances of LinkMgrs has increased to 12, with 4 as the default. This change will have multiple impacts including:

- Support for increased SS7 traffic
- Increased redundancy by supporting more links towards SS7 peers
- Increase the number of peer servers supported per LinkMgr from 256 to 512
- Increase in the number of ASPs per SS7RD from 4 to 12
- Increase in the number of peer servers supported per SS7RD from 144 to 256
- Increase in the number of PSPs per peer server from 4 to 12
Handling of Delete Bearer Request During Inter-SGSN Handoff

**Previous Behavior:** Delete Bearer request during Inter SGSN Hand-off at the new SGSN was being queued and was processed once hand-off procedure was completed.

**New Behavior:** Delete Bearer request during Inter SGSN hand-off at the new SGSN is rejected with cause “110 - Temporarily rejected due to hand over procedure in progress”.

**Impact:** An increase in Delete Bearer Response with cause “110” is observed.

Handling of Suspend-Resume Request from BSC in 2G S4 SM

**Previous Behavior:** Suspend, resume, radio status bad and ready were not handled from the BSC in a 2G S4 SM.

**New Behavior:** The software has been enhanced so that Suspend, resume, radio status bad and ready are now handled from the BSC in a 2G S4 SM.

Handling of Update PDP Request Modified

**Previous Behavior:** The Update PDP request during new SGSN-SRNS procedure was rejected with “no resources available”.

**New Behavior:** The Update PDP request during new SGSN-SRNS procedure is queued and taken up after the completion of DT RAU procedure.

Inclusion or Exclusion of Common Flags IE in CPCQ/UPCQ

**Previous Behavior:** The `gtpc` command under SGTP Service Configuration Mode is used to include/exclude common flags IE in CPCQ/UPCQ. The dual PDP feature over-rides this CLI command, when the dual PDP feature is enabled, IE is always included in CPCQ. If NRSPCA is enabled, the common flags IE in CPCQ are sent even if it is disabled in the SGTP Service Configuration.

**New Behavior:** Inclusion or exclusion of common flags in CPCQ/UPCQ is decided based on the following configurations:

- Common flags will be included if any of the following features are enabled, even if inclusion of common flags is disabled by the `gtpc` command in the SGTP Service Configuration Mode:
  - Dual PDP feature
  - NRSPCA feature
- If none of the above mentioned features are enabled, common flags are included or excluded based on the configuration enabled through the `gtpc` command in the SGTP Service Configuration Mode.

Increased SCTP Associations per Peer RNC

**Previous Behavior:** The maximum number of SCTP associations the SGSN supported per peer RNC was 4.

**New Behavior:** The maximum number of SCTP associations the SGSN supports per peer RNC is now 12; enabling the customer to configure more SCTP connections per peer. The increase in the number of SCTP connections is proportional to the increase in the PSP instances inside the peer server, as indicated in the *Enhancing Link Management Mechanisms* feature change description.

Increasing Number of SS7 Peers Connected per SS7RD
The number of SS7 peers supported per SS7RD has been increased in support of carriers moving to provide Internet-high speed packet access (iHSPA). This change is an integral segment of the scaling redesign of the link management mechanism.

**Previous Behavior:** SGSN currently supports max of 144 peers per SS7RD and max of 256 peers per LinkMgr.

**New Behavior:** SGSN now supports a maximum of 256 SS7 peers per SS7RD and a maximum of 512 SS7 peers per LinkMgr.

### Initiation of a New Signaling Message Towards GGSN

**Previous Behavior:** When “Loss of Radio Coverage” feature is enabled on SGSN, in the case of Intra-RAU, with PLMN change in PMM_IDLE state, the GGSN was not informed of the MS being back in radio coverage after RAU completion.

**New Behavior:** Update PDP Context Request is initiated after RAU accept to inform the GGSN that the UE is back in radio coverage.

### Last Known Location of Subscriber

**Previous Behavior:** There was no last RAI information available to operator for detached subscribers.

**New Behavior:** Last known location of a detached subscriber is stored in the subscriber’s database structure and can now be viewed by the operator in the output of the `show subscribers` command.

### License Control for MOCN Network Sharing

**Previous Behavior:** Network sharing was not a license controlled feature.

**New Behavior:** With the release of 15.0, both 2G and 3G MOCN functionality is now license controlled and the license is required to use all previously available network sharing configuration commands, e.g., network-sharing commands for cs-ps coordination and failure code in the IuPS Service configuration mode. For details, contact your Cisco Account Representative.

### Lower Limit of Implicit Detach Timeout (IDT) Timer Modified

**Previous Behavior:** The lower configurable limit of the Implicit Detach Timeout (IDT) timer is “1” second.

**New Behavior:** The lower configurable limit of the IDT timer is updated to “240” seconds. The Implicit Detach Timeout (IDT) timer is configured through the `gmm` command in SGSN Service Configuration Mode.

For more information on the `gmm` command refer to Cisco ASR 5x00 Command Line Interface Reference.

### Lower Limit Validation For ‘sctp-max-out-strms’

**Previous Behavior:** A crash occurs when “sctp-max-out-strms” is configured to a value less than “2”.

**New Behavior:** If “sctp-max-out-strms” is configured to a value less than “2”, a warning message is displayed and “sctp-max-out-strms” is set to the default value of “2”. The warning message displayed when the value “sctp-max-out-strms” is configured less than “2”:

**Warning:** Value below 2 is not permitted; Default value set is 2

### Modify Bearer Request Suppressed During an ISR Intra RAU Scenario (no change in SGW)

**Previous Behavior:** In release 14.0 if ISR is active, the modify bearer request is triggered with S4-SGSN U-TEID for every Intra-RAU request (that is, without SGW change), to avoid dual paging during Downlink Data notification. When a Modify Bearer Request is sent to SGW with SGSN S4U TEID, it indicates that the subscriber is currently with the...
SGSN and if the SGW receives downlink data it can send the GTPU packet directly to SGSN instead of sending Downlink Data Notifications to both SGSN and MME. When Downlink Data Notifications are sent to both SGSN and MME, paging is triggered at both SGSN and MME. In some cases an Intra-RAU can be followed by an Iu release if there are no follow on requests and the SGSN will send a Release Access Bearer to SGW. This results in additional signaling.

New Behavior: The following behavior changes are implemented in this release:

- The SGSN will not send Modify Bearer Request to SGW if an Intra-RAU follows an ISR activation (provided the Intra RAU does not change the Serving PLMN / RAT Type and there is no change in SGW)
- The SGW will send Downlink Data Notification if it receives any downlink GTPU packet.
- The release 15.0 SGW supports staggered paging. Downlink Data Notification is sent by the SGW in a staggered manner, first to the last known node and then to other node. This avoids dual paging.

Due to the changes listed above Modify Bearer Request is no longer triggered during an ISR Intra RAU scenario.

New counter to Peg Location Report Drop Statistics

Previous Behavior: No counters present to peg the drop statistics of Location Report.

New Behavior: A new counter is added to the show command `show gmm-sm statistics iups-service verbose` to count the Location Report Drop Statistics.

New Counters To Peg Rejects of Authentication and Ciphering Response

Previous Behavior: Counters are present to peg Reject of Authentication and Ciphering response due to the following reasons:

- XRes mismatch
- Too many Sync failure
- Too many Mac failure
- GSM Auth Unacc
- Sync does not have AUTS

New Behavior: Counters have been added to the show command `show gmm-sm statistics verbose` to peg the Authentication and Ciphering response reject due to reasons other than the ones mentioned above. New counters are introduced for 2G and 3G scenarios.

New Traps Added

Previous Behavior: The existing system does not support “CISCO-ENTITY-REDUNDANCY-MIB” traps.

New Behavior: The new system has support for “CISCO-ENTITY-REDUNDANCY-MIB” traps.

Impact: Support for “CISCO-ENTITY-REDUNDANCY-MIB” traps now available.

Optimizing SS7RD Route Structure

Various changes have been made to optimize route structures and memory usage.

Previous Behavior: Using the `no peer-server id instance` command caused the removal of the peer server from the configuration. All remote routes via the peer server were not removed.
New Behavior: Using the `no peer-server id instance` command now removes both the peer server and all routes associated with this peer server from the configuration and operation. A warning message will be displayed prior to removing the peer server and routes.

‘Prohibit payload compression’ Bit Removed From SGSN Initiated UPCQ

Previous Behavior: It is observed that in some scenarios the SGSN was sending “Prohibit payload compression” bit present in Common flags of UPCQ towards the GGSN.

New Behavior: The “Prohibit payload compression” bit is defined only for GGSN initiated messages like CPCR, UPCR from GGSN and UPCQ from GGSN. The SGSN need not send the “Prohibit payload compression” bit. The “Prohibit payload compression” bit will no longer be present in SGSN initiated UPCQ.

Removal of Access Restriction Data Modified

Previous Behavior: Removal of `access-restriction-data` from a call-control-profile provides the option to remove either `eutran-not-allowed` or `failure-code`. Removal of `failure-code` from `access-restriction-data` pops up the following warning:

> Warning: failure-code keyword is deprecated while removing ard configuration. Entire ard configuration is removed

Prior to introduction of this enhancement, removal of `failure-code` was the only option. So entire ARD configuration was warned to be removed.

New Behavior: Removal of `access-restriction-data` from call-control-profile now provides option to remove both `eutran-not-allowed` and `failure code`. To remove both `eutran-not-allowed` and `failure code` execute the following command:

`remove access-restriction-data eutran-not-allowed failure-code <cr>`

When the user wants to remove `failure-code` alone, the warning which was displayed in the earlier implementation is no longer displayed.

Removal Of Record-Module

Previous Behavior: The “record-module” can be deleted even when shared configuration policy is configured. This internally affects the policy for all other active modules.

New Behavior: The “record-module” cannot be deleted if shared policies like use-hard disk, remove-file-after-transfer, file-transfer and so on are configured for the module. The shared policies have to be manually removed before deleting the module. The module can be deleted anytime if no shared policies are configured.

Report Subscriber Summary per GTPU Address

Previous Behavior: It was not possible to report subscriber GTPU sessions or statistics per local-address.

New Behavior: With changes to the `show gtpu` command, it is now possible to display active subscriber sessions on each local GTPU address categorized by GTPU service and to display GTPU statistics per local IP address.

Routing Context in M3ua Data Messages

Previous Behavior: Routing context was not inserted in m3ua-data messages.

New Behavior: A new keyword has been introduced in the `routing-context` command. This keyword controls the insertion of routing context in m3ua-data messages.
S4-SGSN Support for Fallback to V1 Cause Code in GTPv2 Context Response

**Previous Behavior:** The SGSN rejects Context Response message with cause code “Fallback to GTP-V1”.

**New Behavior:** If the SGSN accepts a Context Response message with cause code “Fallback to GTP-V1”, it then performs a GTP-v1 SGSN Context Request, Context Response and Context Ack with the peer SGSN to obtain the subscribers MM and PDP contexts.

Security Modes in MM Context

**Previous Behavior:** In case of 2G- 4G handover (new node is MME), the SGSN was sending context response with MM Context Type “105” & Security Mode as “Type 2 - GSM Key,Used Cipher and Quintuplets”. But if the Peer is a MME, SGSN should send Security Mode as “Type 3” in the Context Response.

**New Behavior:** In the above mentioned scenario, the SGSN now sends context response with MM Context Type “106” and Security Mode “Type 3 - UMTS Key and Quintuplets”.

Separate Statistics for Supplementary Services

**Previous Behavior:** The Supplementary Service Statistics messages are displayed as a part of the show command `show gmm-sm statistics`.

**New Behavior:** New show and clear commands have been added to display and clear Supplementary Service Information. Counters related to Supplementary Service are removed from the show command `show gmm-sm statistics`.

SGSN Allows Re-configuration of Mode For Peer-Server

**Previous Behavior:** The mode under Peer-Server configuration is not re-configurable.

**New Behavior:** The mode under Peer-Server configuration is re-configurable as long as routing context is not configured.

SGSN Support of LLC UI PDU (TOM 8 sapi)

**Previous Behavior:** There was no support for TOM8 SAPI in LLC messages.

**New Behavior:** TOM8 SAPI is implemented to support LCS in 2G. BSSGP messages are also implemented.

SM Cause ‘Collision with network initiated request’

In compliance with changes to 3GPP specifications, all forms of the SGSN now support the SM cause “Collision with network initiated request”.

**Previous Behavior:** SM cause “Collision with network initiated request” was not supported.

**New Behavior:** On receiving a corresponding EGTP cause in an EGTP message by SGSN, the SGSN will map the EGTP cause to the SM cause ”Collision with network initiated request”. New stats, listed under Performance Indicator Changes, have been added to track mapping to this SM cause.

SRNS Relocation Feature Enhancement

**Previous Behavior:** The SGSN did not support Intra-SRNS relocation if the source-rnc itself was behaving as the target-rnc.

**New Behavior:** The software has been enhanced so that the SGSN now can be configured to support Intra-SRNS relocation if the source-rnc itself is behaving as the target-rnc.
Support for BGGSP Messages in LCS

**Previous Behavior:** Support for location services-related BGGSP messages was not included.

**New Behavior:** BGGSP messages have been implemented in this release to support location services for the 2G SGSN in compliance with 3GPP TS 3GPP TS 48.018.

Support for Sending origin-node-type IE in UMTS ISR

**Previous Behavior:** Consider the following scenario:
1. Idle-Mode-Signaling Reduction (ISR) is enabled for UMTS network access.
2. Successful 3G-Attach (EPC & ISR capability supported), Activate,
3. Successful Old-SGSN-Israu on S3 interface (ISR activated),
4. SGSN sends Release-Access-Bearer-Request without the origin-node-type IE.

**New Behavior:** The software has been enhanced so that in the above scenario, the origin-node-type IE is sent. The IE will be sent via the S11 interface if ISR is active in the MME. The IE will be sent via the S4 interface if ISR is active in the SGSN.

Support for Smaller SCTP Bundle Timeout

**Previous Behavior:** SCTP bundle timeouts, in the `timeout` command in the `SCTP Parameters Template Configuration Mode` and the `SGSN PSP Configuration Mode`, were configured in units of 100 ms.

**New Behavior:** The software has been enhanced to allow operators to configure SCTP bundle timeouts in units of 10 ms. These changes were made to the `timeout` command in `SCTP Parameters Template Configuration Mode` and `SGSN PSP Configuration Mode`.

Support for Vendor-specific-application-id in S6d Interface

**Previous Behavior:** The diameter implementation on SGSN does not send Vendor-Specific-Application-ID Grouped AVP in any diameter application messages.

**New Behavior:** The SGSN now sends Vendor-Specific-Application-Id AVP in all S6d messages from the SGSN.

**Impact:** The intermediate nodes have to decode the Vendor-Specific-Application-Id AVP.

Support to Configure Release Compliance of Standard Dictionary

**Previous Behavior:** Diameter supports three dictionaries Standard, Standard-r9, and custom dictionary. The Standard dictionary is 3GPP TS 29.272 Release 8 compliant and Standard-r9 is 3GPP TS 29.272 Release 9 compliant. The operator could configure the required dictionary.

**New Behavior:** The Standard-r9 and custom dictionaries are no longer supported. There will be only one Standard dictionary. The Standard dictionary which was 3GPP TS 29.272 Release 8 compliant in earlier releases, will now contain AVPs of Release 9 and Release 10 as well. A new CLI command `diameter update-dictionary-avps {3gpp-r10 | 3gpp-r9}` is introduced under the HSS Peer Service Configuration mode, to configure the release that has to be supported for the HSS Peer Service. This new command is applicable only for the Standard dictionary and can be configured as either Release 9 or Release 10 compliant. The default standard dictionary has been retained as Release 8 compliant to ensure backward compatibility. The “no” form of the command can be used to disable the command.

Tariff Time Feature

**Previous Behavior:** The rotation of the EDR record files based on:

- **Volume:** When the file size exceeds the configured volume limit in bytes, the file is rotated.
- **Time**: Specifies the period of time (in seconds) to wait before closing the EDR file and creating a new one.
- **Number of records**: When the number of records stored in the file exceeds the configured limit, the file is rotated.

**New Behavior**: The file command in the in EDR Module Configuration Mode is updated, a new option `tariff-time` is added to the `rotation` keyword in the file command. If this keyword is configured, the files can be rotated once per day at the configured time of the day. The hour and minute at which the files will be rotated can be configured through this option.

### Update PDP Request From GGSN Processed After RAU Procedure

**Previous Behavior**: The Update PDP Request from GGSN during 2G new SGSN ISRAU was rejected.

**New Behavior**: The Update PDP Request from GGSN during 2G new SGSN ISRAU is queued and taken up after completion of RAU procedure.

### SGSN Command Changes as of September 30, 2013

This section provides information on SGSN command changes in release 15.0.

**Important**: For more information regarding commands in this section, refer to the *Cisco ASR 5x00 Command Line Interface Reference* for this release.

### New SGSN Commands

This section identifies new SGSN commands available in release 15.0.

#### clear supplementary-service statistics

New clear command `clear supplementary-service statistics` has been added to clear Supplementary Service Information.

```
[local]host_name# clear supplementary-service statistics
```

#### diameter update-dictionary-avps

A new CLI command `diameter update-dictionary-avps { 3gpp-r10 | 3gpp-r9 }` is introduced under the HSS Peer Service Configuration mode, to configure the release compliance of the Standard dictionary that is supported for the HSS Peer Service. This new command is applicable only for the Standard dictionary and can be configured as either Release 9 or Release 10 compliant. The default standard dictionary has been retained as Release 8 compliant to ensure backward compatibility. The “no” form of the command can be used to disable the command.

```
config

    context <context_name>

    hss-peer-service <service_name>

    diameter update-dictionary-avps { 3gpp-r10 | 3gpp-r9 }

end
```
**gprs-mocn**

The new `gprs-mocn` command, in the SGSN-Global configuration mode, enables network sharing for GPRS multi-operator core network (2G MOCN):

```plaintext
config
  sgsn-global
    gprs-mocn
    no gprs-mocn
  end

Note:
- When `no` is used with this command, the configuration reverts to the default status and GPRS MOCN is disabled.

For additional information, refer to the 2G SGSN Multi-Operator Core Network chapter in the Serving GPRS Support Node Administration Guide.

**inter-rnc-procedures source-rnc-as-target**

A new command has been added to Iups Service Configuration Mode to allow operators the ability to enable SRNS relocation for those scenarios where the source RNC is behaving as the target RNC. The default behavior is to disable SRNS relocation in those scenarios.

```plaintext
config
  context context_name
    iups-service iups_service_name
      inter-rnc-procedures source-rnc-as-target
      no inter-rnc-procedures source-rnc-as-target
    end

Note:
- `no` disables the ability of the SGSN to process SRNS relocation when the source RNC is behaving as the target RNC.

**network-sharing cs-ps-coordination**

The `network-sharing cs-ps-coordination` enables or disables the cs-ps coordination check for homer or roamer. It is also used to set the failure code that will be sent while the SGSN is requesting the BSC to provide CS-PS coordination.

The operator should configure cs-ps-coordination checking explicitly for homer or roamer subscribers and for the failure-code to be sent when the SGSN asks the BSC to perform CS-PS coordination.

```plaintext
config
```
context <ctxt_name>

gprs-service <gprs_svc_name>

    network-sharing cs-ps-coordination [ roamer | homer | failure-code <gmm-cause> ]

end

Notes: Variations of the network sharing command can be used to adjust the CS-PS configuration.

- network-sharing cs-ps-coordination failure-code <gmm-cause> – sets the gmm cause value to be sent only when rejecting the Attach/RAU Request with the cause cs-ps-coordination is required. This setting applies to both homer and roamer. Default is 14.
- default network-sharing cs-ps-coordination – sets the cs-ps-coordination parameters to default. By default, checking for cs-ps-coordination is enabled for homer and roamer.

**network-sharing failure-code**

The following command sequence sets the failure code that is used by GPRS MOCN if no failure cause is available when the SGSN sends a Reject message

```plaintext
config

    context <ctxt_name>

    gprs-service <gprs_svc_name>

        network-sharing failure-code <gmm-cause>

end
```

Default network sharing failure-code is 7.

**plmn id**

In support of 2G MOCN network sharing functionality, new keywords are added to the `plmn id` command to define the common PLMN-Id and an optional list of dedicated PLMN-Ids in the GPRS service.

```plaintext
config

    context <ctxt_name>

    gprs-service <gprs_svc_name>

        plmn id mcc <mcc_id> mnc <mnc_id> [ network-sharing common-plmn mcc <mcc_id> mnc <mnc_id> [ plmn-list mcc <mcc_id> mnc <mnc_id> [ mcc <mcc_id> mnc <mnc_id> ] + ] ]

end
```

Notes:
• + in the syntax above indicates that the mcc/mnc combination can be repeated as often as needed to define all PLMN-Ids needed in the list.

pool

A new pool command has been provided in the eGTP Service Configuration, to enable flex pooling (Lu/Gb over S16) support on the S4-SGSN.

```
config

context <context_name>

egtp-service <service_name>

pool { default-sgsn | hop-counter <count> }

no pool default-sgsn

end
```

show sgsn fsm-statistics

The following command tracks 3G SGSN (both Gn and S4) application FSM statistics. 2G FSM statistics are not yet supported on the SGSN.

```
show sgsn fsm-statistics { umts-sm | umts-pmm | all }
```

Notes:
- all: Displays all SGSN application FSM statistics.
- umts-pmm: Displays 3G Mobility Management PMM FSM statistics.

show supplementary-service statistics

New show command `show supplementary-service statistics` has been added to display Supplementary Service Information.

```
[local]host_name# show supplementary-service statistics
```

Modified SGSN Commands

This section identifies SGSN commands modified in release 15.0.

accounting

The accounting command in GPRS Service Configuration Mode and SGSN Service Configuration Mode has been updated to include a new keyword lcs mo-cdr, to enable/disable the generation of LCS-MO-CDRs.

```
config

context <context_name>
```
The following command sets up an Application Server Process (ASP) instance in the SS7RD configuration:

```
config
  ss7-routing-domain <rd_id> variant <variant_type>
  asp instance <asp_inst>
end
```

Notes:
- `asp instance <asp_inst>` identifies an ASP instance in the SS7RD configuration. The valid instance range has increased from 1-4 to 1-12.

**edr-module active-charging-service [ charging | reporting ]**

In releases prior to 15.0, the SGSN re-used the existing ‘EDR’ module for generating event logs which is primarily used for charging records. But from release 15.0 onwards, the session-event module is used by SGSN for event logging. For more information see the `session-event-module` command.

```
config
  context <context_name>
    [no] edr-module active-charging-service [ charging | reporting ]
end
```

**file**

The file command is updated to include a new option `tariff-time` for the keyword `rotation` to configure the EDR file rotation time once per day.

```
config
```
context `<context_name>`

   edr-module active-charging-service [ charging | reporting ]

   file [ charging-service-name { include | omit } ] [ compression { gzip | none } ] [ current-prefix string ] [ delete-timeout seconds ] [ directory directory_name ] [ edr-format-name ] [ exclude-checksum-record ] [ field-separator { hyphen | omit | underscore } ] [ file-sequence-number rulebase-seq-num ] [ headers ] [ name file_name ] [ reset-indicator ] [ rotation { num-records number | tariff-time minute minute_value hour hour_value | time seconds | volume bytes } ] [ sequence-number { length length | omit | padded | padded-six-length | unpadded } ] [ storage-limit limit ] [ single-edr-format ] [ time-stamp { expanded-format | rotated-format | unix-format } ] [ trailing-text string ] [ trap-on-file-delete ] [ xor-final-record ]

   default file [ charging-service-name ] [ compression ] [ current-prefix ] [ delete-timeout ] [ directory ] [ edr-format-name ] [ field-separator ] [ file-sequence-number ] [ headers ] [ name ] [ reset-indicator ] [ rotation { num-records | tariff-time | time | volume } ] [ sequence-number ] [ storage-limit ] [ time-stamp ] [ trailing-text ]

   end

gmm implicit-detach-timeout

This command is now supported for the 2G Idle Mode Signaling Reduction (ISR) feature in GPRS Configuration Mode. In addition, the lower configurable limit of the gmm implicit-detach-timeout value has been changed from 1 to 240 seconds. This change is made to allow a 4 minute gap between the implicit detach timeout value and the gmm T3323 timeout value used for 3G ISR, as one timer is updated with regard to the other.

config

   context `<plmn_name>`

   gprs-service `<gprs_service_name>`

   gmm implicit-detach-timeout `<secs>`

   end

Note:

- Use this command in conjunction with the idle-mode-signaling-reduction access-type gprscommand in Call Control Profile Configuration Mode to fully configure the 2G ISR feature.

gtp suppress-cdrs zero-volume

This command suppresses the CDRs with zero byte data count. The CDRs can be classified as Final-cdrs, Internal-trigger-cdrs, and External-trigger-cdrs. This command provides an option to select the CDRs to be suppressed. This command is disabled by default.

config

   context `<context_name>`
Idle Mode Signaling Reduction Access Type

The `gprs` keyword has been added to this command to provide the option to enable 2G network access for the Idle Mode Signaling Reduction (ISR) feature.

```bash
config
    call-control-profile <profile_name>
        idle-mode-signaling-reduction access-type gprs
    end
```

Note:
- After enabling 2G ISR with the `gprs` keyword, use the `gmm implicit-detach-timeout` command in GPRS Service Configuration Mode to specify the implicit detach timeout value to use for 2G ISR.

Lawful Intercept

The `allow-direct-tunnel` keyword has been added to this command to enable 3G subscriber LI targets to continue in Direct Tunnel mode rather than 2-tunnel mode. For more information on Lawful Intercept, contact your Cisco representative.

Map Message

This Call Control Profile Configuration Mode command is enhanced with the `mo-fwd-sm` keyword so operators can instruct the SGSN to include the IMSI of the originating subscriber in the mobile-originated SM transfer.

```bash
config
    call-control-profile <cc_profile_name>
        map message mo-fwd-imsi
        remove map message mo-fwd-imsi
    end
```

Note:
- The system default is not to include the IMSI.
- `remove` disables the inclusion of the IMSI.

Network-Initiated PDP Activation

The new `secondary` keyword has been added to the `network-initiated-pdp-activation` command in the Call Control Profile mode. The `secondary` keyword specifies that only network-initiated secondary PDP context activations (NRSPCAs) are to be allowed.
config

call-control-profile <profile_name>

  network-initiated-pdp-activation secondary access-type <gprs | umts> { all failure-code <failure_code> | location-area-list instance <instance> failure-code <failure_code> }

end

Notes:
- To enable NRSPCA, you must also enable the common flags IE with the gtpc send command in the SGTP Service configuration mode.
- remove added to the command disables NRSPCA by removing the network-initiated-pdp-activation definition from the configuration.
- There is no default form of the command.

network-sharing cs-ps-coordination

The new homer and roamer filters enable (default) the operator to configure homer/roamer differentiation for 3G SGSN cs-ps coordination.

config

  context <context_name>

    iups-service <service_name>

    network-sharing cs-ps-coordination [ homer | roamer ]

end

Notes:
- default resets the SGSN default to enable checking for cs-ps-coordination for a 3G SGSN.
- no removes the configuration definition, thus disabling cs-ps-coordination checking for a 3G SGSN.
- homer enables checking for cs-ps-coordination for homers only (UE in its home network) or a 3G SGSN.
- roamer enables checking for cs-ps-coordination for roamers only (UE from outside the home network) for a 3G SGSN.

session-event-module

From release 15.0 onwards, the session-event module is used by SGSN for event logging. By default, EDR files are generated at the location: /hd-raid/records/edr. After upgrading to release R15.0, if this CLI is configured, the path for EDR files changes to: /hd-raid/records/event.

config

  context <context_name>

    [no] session-event-module
network-initiated-pdp-activation

The `secondary` keyword has been added to the `network-initiated-pdp-activation` command in the Call Control Profile mode. The `secondary` keyword specifies that only network-initiated secondary PDP context activations (NRSPCAs) are to be allowed.

```
config
  call-control-profile <profile_name>
    network-initiated-pdp-activation allow secondary access-type
  end

peer-server

The following command sets up a peer-server instance in the SS7RD configuration:

```
config
  ss7-routing-domain <rd_id> variant <variant_type>
    peer-server id <srvr_id>
  end

Notes:
- `peer-server id <srvr_id>` identifies the instance is a peer-server configuration in the SS7 routing domain. The valid Id range has increased from 1-144 to 1-256.

pssp

The following command sets up a Peer Server Process (PSP) instance in the SS7RD configuration:

```
config
  ss7-routing-domain <rd_id> variant <variant_type>
    peer-server id <srvr_id>
      psp instance <psp_inst>
    end

Notes:
- `psp instance <psp_inst>` identifies a PSP instance in the SS7RD configuration. The valid instance range has increased from 1-4 to 1-12.

ranap paging-cause-ie mme-signalling

The command `ranap paging-cause-ie mme-signalling < paging_cause_value >` is used to set the Paging Cause IE value for paging from MME due to Circuit Switch Fallback (CSFB).
config

  context <context_name>

    iups-service <iups_service_name>

    rnc id <rnc_id>

    [default | no ] ranap paging-cause-ie mme-signalling <paging_cause_value >

end

Where:

- The command ranap paging-cause-ie mme-signalling < paging_cause_value > is used to set the Paging Cause IE value for paging from MME due to Circuit Switch Fallback (CSFB). Listed below are the paging cause values which can be set:
  - 0 - Terminating conversational call
  - 1 - Terminating streaming call
  - 2 - Terminating interactive call
  - 3 - Terminating background call
  - 4 - Terminating low priority signaling
  - 5 - Terminating high priority signaling
- The default command resets the specific parameters value to default. In this case it is set to “5 - Terminating high priority signaling”.
- The no form of the command suppresses the Paging Cause IE so that it is not included in responses to Paging Requests.

routing-context

A new keyword m3ua-data is included in the routing-context command. This keyword controls the insertion of routing context in outbound M3UA data messages. The default behavior is to insert routing context in management messages and suppress routing context in data messages.

config

  ss7-routing-domain <index_name>

    peer-server<peer_server_id>

    psp<psp_instance>

    routing-context { discard-inbound | process-inbound | m3ua-data

    { insert-outbound | suppress-outbound } }

end

show gtpu

There are two new keywords related to displaying information per local addresses for GTPU services.
show gtpu { local-addresses | statistics [ [ gtpu-service <srvc_name> ] [ gtpumgr-instance <instance> ] [ local-address <ip_address> ] | [ peer-address <ip_address> ] ] [ | { grep <grep_options> | more } ] }

Notes:
- show gtpu local-addresses Displays number of active sessions on all local-addresses in all GTPU services.
- show gtpu statistics local-address <ip_address> Displays subscriber information per local GTPU address in a GTPU service.
- <ip_address> Can be any valid IPv4 or IPv6 address.

**task**

The following command controls the maximum number of LinkMgrs that can be configured:

```plaintext
config
  task facility linkmgr max <number>
end
```

**Important:** This value must be set before configuring any SGSN service-related configurations. This command cannot be set dynamically. If the LinkMgr count is modified dynamically, the system must be rebooted for the change to take effect.

Notes:
- The maximum number of linkmgrs has increased from 4 to 12, keeping a default of 4.

**timeout**

Multiple keywords have been added to the `timeout` command in the LCS service in support of the expanded LCS functionality:

```plaintext
config
  context <context_name>
    location-service <location_svc_name>
      timeout { area-event-invoker-timer <aitertimeout_seconds> | lcsn <lcsn_seconds> | periodic-event-invoker-timer <petimeout_seconds> | ue-available-guard-timer <ueagtimer_seconds>
      }
end
```

Notes:
- `area-event-invoker-timer` - used to guard the area event invoke procedures. Valid range is 10 to 20 seconds; default is 15.
- `lcsn` - sets NAS location notification timer (introduced in Release 14.0). Valid range is 10 to 20 seconds; default is 15.
• **periodic-event-invoke-timer** - used to guard the period location invoke procedure. Valid range is 10 to 20 seconds; default is 15.

• **ue-available-guard-timer** - used to guard packet-switched deferred location request (UE available event) procedures. Valid range is 10 to 600 seconds; default is 600.

• **default timeout** resets the timer default value(s).

### Deprecated SGSN Commands

This section identifies deprecated SGSN commands that are no longer supported in release 15.0.

None for this release.

### SGSN Performance Indicator Changes as of September 30, 2013

This section provides information on SGSN performance indicator changes in release 15.0.

👩‍🏫 **Important:** For more information regarding bulk statistics and output fields and counters in this section, refer to the *Cisco ASR 5x00 Statistics and Counters Reference* for this release.

### New SGSN Bulk Statistics

This section identifies new SGSN bulk statistics available in release 15.0.

### New in the SGSN Schema

These new gauges track UEs that support or do not support network sharing:

- 2G-network-sharing-supp-ue
- 2G-network-sharing-non-supp-ue

With the behavior change supporting SM cause "Collision with network initiated request", the following new stats track the SGSN mapping an EGTP cause to the SM cause.

- 3G-sec-actv-rej-coll-with-net-init-req
- 2G-sec-actv-rej-coll-with-net-init-req

The following new statistics have been added in support of tracking and monitoring S4 functionality:

- 2G-total-num-actv-pdp-on-s4
- 3G-total-num-actv-pdp-on-s4
- 2G-num-subs-with-isr
- 3G-num-subs-with-isr
- 2G-num-sgw-reloc-due-to-intra-rau
- 3G-num-sgw-reloc-due-to-intra-rau
- 2G-num-sgw-reloc-due-to-s16-ra
- 3G-num-sgw-reloc-due-to-s16-ra
• 2G-num-sgw-reloc-due-to-s3-rau
• 3G-num-sgw-reloc-due-to-s3-rau

In support of the new SM cause code, two new bulk statistics have been added:
• 3G-sec-actv-rej-coll-with-net-init-req
• 2G-sec-actv-rej-coll-with-net-init-req

Modified SGSN Bulk Statistics
This section identifies SGSN bulk statistics modified in release 15.0.
None for this release.

Deprecated SGSN Bulk Statistics
This section identifies deprecated SGSN bulk statistics that are no longer supported in release 15.0.
None for this release.

New SGSN Output Fields and Counters
This section identifies new SGSN show command output fields and counters available in release 15.0.

show bssgp statistics [ verbose ]
BGGSP messages have been implemented in this release to support location services for the 2G SGSN:
• LCS Messages
• Perform Location Request transmitted
• Position Command received
• Position Response transmitted
• Perform Location Response received
• Perform Location Abort transmitted
• Perform Location Request dropped
  • due to LCS not supported
  • due to BVCI not found
• Perform Location Abort dropped
  • due to LCS not supported
  • due to BVCI not found
• Position Response dropped
  • due to LCS not supported
  • due to BVCI not found Position Command dropped
  • due to LCS not supported
- due to Subscriber unknown
- due to BVCI not found
- due to blocked BVCI
- Perform Location Response dropped
  - due to LCS not supported
  - due to Subscriber unknown

**show configuration**

The output of this command has been enhanced to show whether 2G ISR is enabled, and whether the `gmm implicit-detach-timeout` value has been configured.

- `context <context_name>`
  - idle-mode-signaling-reduction access-type gprs
- `context <context-name>`
  - gmm implicit-detach-timeout `<value>`

**show call-control-profile full name `<profile_name>`**

The output of this command has been enhanced to indicate if 2G ISR is enabled in the Call Control Profile.

- Idle-Mode-Signaling-Reduction (ISR) for GPRS:
  - MAP MO-FWD-SM Message. Include IMSI:
    - A new field appears in the output of this command to indicate if the SGSN is configured to include the IMSI of the originating subscriber in the mobile-originated SM transfer.
    - MAP MO-FWD-SM Message. Include IMSI:

**show configuration, show configuration verbose, show configuration context, show configuration context verbose**

New statistics have been introduced to support LCS-MO-CDRs.

- Under GPRS Service, “lcs mo-cdr” is displayed as a accounting cdr type.
- Under SGSN Service, “lcs mo-cdr” is displayed as a accounting cdr type.

**show gmm-sm statistics**

New counters are added to count invalid imsi-detach-requests.

- Dropped-Detach-Req
- 3G-MS-Init-IMSI-Detach-Req-During-actv/sms-auth-ongoing

Two new counters in the command output indicate the total number of currently activated 2G ISR subscribers:

- ISR Activated Subscribers:
• 2G Intra RAU with SGW Relocation

**show gmm-sm statistics iups-service verbose**

New counter added to count Location Report Drop Statistics.

• Location Report Dropped

**show gmm-sm statistics sm-only**

The following counters are included in the `show gmm-sm statistics sm-only` command output to support the NRSPCA feature.

**Table 1. NRSPCA SM Statistics**

<table>
<thead>
<tr>
<th>NRSPCA SM Statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Activate Context Request</strong></td>
</tr>
<tr>
<td>Actv-Request-Nrspca</td>
</tr>
<tr>
<td>3G-Actv-Request-Nrspca</td>
</tr>
<tr>
<td>2G-Actv-Request-Nrspca</td>
</tr>
<tr>
<td><strong>Activate Context Request Retransmitted</strong></td>
</tr>
<tr>
<td>3G-Secondary-Actv-Drop-Nrspca</td>
</tr>
<tr>
<td>2G-Secondary-Actv-Drop-Nrspca</td>
</tr>
<tr>
<td><strong>Activate Context Accept</strong></td>
</tr>
<tr>
<td>Actv-Accept-Nrspca</td>
</tr>
<tr>
<td>3G-Actv-Accept-Nrspca</td>
</tr>
<tr>
<td>2G-Actv-Accept-Nrspca</td>
</tr>
<tr>
<td><strong>Activate Context Reject</strong></td>
</tr>
<tr>
<td>Actv-Reject-Nrspca</td>
</tr>
<tr>
<td>3G-Actv-Reject-Nrspca</td>
</tr>
<tr>
<td>2G-Actv-Reject-Nrspca</td>
</tr>
<tr>
<td><strong>Request Secondary Pdp Context Activation</strong></td>
</tr>
<tr>
<td>Total-Request-Sec-Pdp-Ctxt-Req</td>
</tr>
<tr>
<td>3G-Request-Sec-Pdp-Ctxt-Req</td>
</tr>
<tr>
<td>2G-Request-Sec-Pdp-Ctxt-Req</td>
</tr>
<tr>
<td><strong>Retransmission</strong></td>
</tr>
<tr>
<td>Total-Request-Sec-Pdp-Ctxt-Req</td>
</tr>
<tr>
<td>3G-Request-Sec-Pdp-Ctxt-Req</td>
</tr>
<tr>
<td>2G-Request-Sec-Pdp-Ctxt-Req</td>
</tr>
<tr>
<td><strong>Request Secondary Pdp Context Activation Reject</strong></td>
</tr>
<tr>
<td>Total-Request-Sec-Pdp-Ctxt-Reject</td>
</tr>
<tr>
<td>3G-Request-Sec-Pdp-Ctxt-Reject</td>
</tr>
<tr>
<td>2G-Request-Sec-Pdp-Ctxt-Reject</td>
</tr>
<tr>
<td><strong>Request Secondary Pdp Context Activation Denied</strong> (verbose only)</td>
</tr>
</tbody>
</table>
### NRSPCA SM Statistics

<table>
<thead>
<tr>
<th>3G-Insufficient Resources</th>
<th>2G-Insufficient Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>3G-Actv Rej Unspecified</td>
<td>2G-Actv Rej Unspecified</td>
</tr>
<tr>
<td>3G-Feature Not Supported</td>
<td>2G-Feature Not Supported</td>
</tr>
<tr>
<td>3G-Sem Err in TFT OP</td>
<td>2G-Sem Err in TFT OP</td>
</tr>
<tr>
<td>3G-Syntactic Err in TFT OP</td>
<td>2G-Syntactic Err in TFT OP</td>
</tr>
<tr>
<td>3G-Unknown Ctx</td>
<td>2G-Unknown Ctx</td>
</tr>
<tr>
<td>3G-Sem Err in Pkt Filter</td>
<td>2G-Sem Err in Pkt Filter</td>
</tr>
<tr>
<td>3G-Syntactic Err in Pkt Filter</td>
<td>2G-Syntactic Err in Pkt Filter</td>
</tr>
<tr>
<td>3G-Ctx No-Tft Already Activated</td>
<td>2G-Ctx No-Tft Already Activated</td>
</tr>
<tr>
<td>3G-Actv Rej BCM violation</td>
<td>2G-Actv Rej BCM violation</td>
</tr>
<tr>
<td>3G-Proto Err Unspecified</td>
<td>2G-Proto Err Unspecified</td>
</tr>
</tbody>
</table>

### Request Secondary Pdp Context Activation Rejects Dropped

| 3G-Request-Sec-Pdp-Ctxt-Rej-Dropped | 2G-Request-Sec-Pdp-Ctxt-Rej-Dropped |

### Request Secondary Pdp Context Activation Aborted

<table>
<thead>
<tr>
<th>3G-NRSPCA-Abort-Subs-Detach</th>
<th>2G-NRSPCA-Abort-Subs-Detach</th>
</tr>
</thead>
<tbody>
<tr>
<td>3G-NRSPCA-Abort-Linked-Ctx-Deactv</td>
<td>2G-NRSPCA-Abort-Linked-Ctx-Deactv</td>
</tr>
<tr>
<td>3G-NRSPCA-Abort-Max-Retry-Attempts</td>
<td>2G-NRSPCA-Abort-Max-Retry-Attempts</td>
</tr>
<tr>
<td>3G-NRSPCA-Abort-Paging-Expiry</td>
<td>2G-NRSPCA-Abort-Paging-Expiry</td>
</tr>
<tr>
<td>3G-NRSPCA-Abort-Subs-Suspend</td>
<td>2G-NRSPCA-Abort-Subs-Suspend</td>
</tr>
<tr>
<td>3G-NRSPCA-Abort-Handoff</td>
<td>2G-NRSPCA-Abort-Handoff</td>
</tr>
<tr>
<td>3G-NRSPCA-Abort-Inter-RAT-Handoff</td>
<td>2G-NRSPCA-Abort-Inter-RAT-Handoff</td>
</tr>
<tr>
<td>3G-NRSPCA-Abort-Intra-RAU</td>
<td>2G-NRSPCA-Abort-Intra-RAU</td>
</tr>
<tr>
<td>3G-NRSPCA-Abort-SRNS-Handoff</td>
<td>2G-NRSPCA-Abort-SRNS-Handoff</td>
</tr>
<tr>
<td>3G-NRSPCA-Abort-Intra-SRNS</td>
<td>2G-NRSPCA-Abort-Intra-SRNS</td>
</tr>
<tr>
<td>3G-NRSPCA-Abort-RAB-Failure</td>
<td>2G-NRSPCA-Abort-RAB-Failure</td>
</tr>
<tr>
<td>3G-NRSPCA-Abort-Ctx-Deactv</td>
<td>2G-NRSPCA-Abort-Ctx-Deactv</td>
</tr>
</tbody>
</table>

### Secondary Pdp Context Activation Request Ignored (verbose only)

<table>
<thead>
<tr>
<th>Total-Actv-Request-Nrspca-Ignored</th>
<th>2G-Actv-Request-Nrspca-Ignored</th>
</tr>
</thead>
<tbody>
<tr>
<td>3G-Actv-Request-Nrspca-Ignored</td>
<td></td>
</tr>
</tbody>
</table>

### show gmm-sm statistics verbose

New counters are added to count the number of Authentication and Ciphering Response rejects due to reasons which are not previously listed.

- 3G-Other cause
- 2G-Other cause

A new counter, has been added to the *Forward Relocation Reject Causes* section of the `show gmm-sm statistics verbose` command output.

- Invalid Core Network Interface

This counter will be incremented each time a gtpv2-forward-relocation-request message is received and the `sgsn-core-nw-interface` is configured as `gn`.

- GPRS MOCN Attach Statistics
• Total Redirection Attempts Rcvd:
• Redirection attempts rcvd with bssgp imsi:
• Redirection attempts rcvd without bssgp imsi:
• Total Redirection Completes Sent:
• Successful Redirection completes sent:
• Failure Redirection completes sent:
• Total Redirection Indications Sent:
• Illegal PLMN:
• Illegal LA:
• No roaming:
• No gprs PLMN:
• No cell in LA:
• CS/PS Coord Rqr:
• Others:

• GPRS MOCN RAU Statistics
  • Total Redirection Attempts Rcvd:
  • Redirection attempts rcvd with bssgp imsi:
  • Redirection attempts rcvd without bssgp imsi:
  • Total Redirection Completes Sent:
  • Successful Redirection completes sent:
  • Failure Redirection completes sent:
  • Total Redirection Indications Sent:
  • Illegal PLMN:
  • Illegal LA:
  • No roaming:
  • No gprs PLMN:
  • No cell in LA:
  • CS/PS Coord Rqr:
  • Others:

show gprs-service name <service-name>

New fields in the output of this command indicate configured information for 2G MOCN:

• Network Sharing
• Common Plmn-id
• Local PLMNS
- PLMN
- CS/PS Co-ordination homer
- CS/PS Co-ordination roamer
- CS/PS Co-ordination failcode
- Network-sharing Failure-code

**show gprs-service all**

New statistics have been introduced to support LCS-MO-CDRs.

- Accounting cdr-types : lcs mo-cdr

**show gtpp counters all**

New statistics have been introduced to support LCS-MO-CDRs.

- Outstanding LCS-MO-CDRs
- Possibly Duplicate Outstanding LCS-MO-CDRs
- Archived LCS-MO-CDRs
- LCS-MO-CDRs buffered with AAAPROXY
- LCS-MO-CDRs buffered with AAAMGR

**show gtpp counters cgf-address**

New statistics have been introduced to support LCS-MO-CDRs.

- Outstanding LCS-MO CDRs
- Possibly Duplicate Outstanding LCSM0-CDRs

**show gtpp counters group name**

New statistics have been introduced to support LCS-MO-CDRs.

- Outstanding LCS-MO-CDRs
- Possibly Duplicate Outstanding LCS-MO-CDRs
- Archived LCS-MO-CDRs
- LCS-MO-CDRs buffered with AAAPROXY
- LCS-MO-CDRs buffered with AAAMGR

**show gtpp group**

New statistic added to indicate if suppression of CDRs with zero byte data count has been enabled. When suppression of CDRs with zero byte data count is enabled, it indicates the types of CDRs being suppressed.

- Suppress zero-volume CDRs

**show gtpp statistics, show gtpp statistics cgf-address, show gtpp statistics debug-info, show gtpp statistics group name, show gtpp statistics verbose debug-info**
New statistics have been introduced to support LCS-MO-CDRs.

- Total LCS-MO-CDR transmission
- Total LCS-MO-CDR retransmission
- Total LCS-MO-CDR accepted
- Total LCS-MO-CDR transmission failures
- LCS-MO-CDR transmission failure percent

**show gtpp storage-server statistics, show gtpp storage-server statistics verbose, show gtpp storage-server statistics group name**

New statistics have been introduced to support LCS-MO-CDRs.

- Store Requests (LCS-MO-CDRs)
  - Sent
  - Retried
  - Success
  - Failed

**show hss-peer-service service name**

A new parameter has been added to indicate the configured release compliance of the Standard dictionary used for HSS Peer Service.

- Update-Dictionary-Avps

**show iups-service name <service_name>**

A new parameter is included to display the paging cause IE value set for paging from MME due to Circuit Switch Fallback (CSFB).

- MME-Signalling

A new field has been added to the output of this command to indicate whether or not the SGSN is configured to handle SRNS relocation when the source RNC is behaving as the target RNC.

- Source-RNC as Target-RNC : Not Allowed
- Source-RNC as Target-RNC : Allowed

The output for this command has been modified with new value options for the Check CS/PS Co-ordination field:

- Enabled
- Enabled (Homer Only)
- Enabled (Roamer only)
- Disabled

The previously displayed value options were Continue and Reject

**show linkmgr instance <instance> parser statistics memory**
Two new fields have been added to the output of this command to indicate changes in memory usage associated with this behavior change:

- SS7RD Route entry
- SS7RD RTE ELMNT entry

**show llc statistics verbose**

New fields are included in the output of the `show llc statistics verbose` command in to display LLC IU PDU (TOM8 sapi):

- `rx_frm_tom8_rcvd`
- `tx_frm_tom8_sent`

**show location-services service name <service_name>**

Three new fields indicate the values configured for the new timers set with the `timeout` command for Location-Services:

- UE AVAILABLE GUARD Timer
- AREA EVENT INVOKE Timer
- PERIODIC EVENT INVOKE Timer

**show map statistics name <map-service-name>**

New counters have been added to indicate different failure responses for MAP Provide Subscriber Location responses.

- Provide Subscriber Location Failures - System Failure
- Provide Subscriber Location Failures - Data Missing
- Provide Subscriber Location Failures - Unexpected Data Value
- Provide Subscriber Location Failures - Facility Not Supported
- Provide Subscriber Location Failures - Unidentified Subscriber
- Provide Subscriber Location Failures - Illegal Subscriber
- Provide Subscriber Location Failures - Illegal Equipment
- Provide Subscriber Location Failures - Absent Subscriber
- Provide Subscriber Location Failures - Unauthorized Requesting Network
- Provide Subscriber Location Failures - Unauthorized LCS Client
- Provide Subscriber Location Failures - Position Method Failures

**show s4-sgsn statistics**

The output of this command is enhanced to provide information on the various reasons for deactivations of ISR-activated 2G subscribers.

- 2G Intra RAU with SGW Relocation
- Detach Notification from MME to 2G
• 2G MS Initiated Detach
• 2G Cancel Location from HSS/HLR
• 2G Local Admin Detach
• 2G Implicit Detach Timer Expiry

The output of this command has also been enhanced to provide a counter that increments when a PDP is removed upon receiving a Delete Bearer Request (DBR) from a New SGW during Intra-SRNS relocation. This scenario can occur if the DBR is initiated from a New SGW before a Modify is received at its end.

• PDP Deletion Statistics:
  • DBR from new SGW during Intra SRNS:

show session disconnect-reasons verbose

The following new disconnect reasons have been added in support of the new Network Requested Secondary PDP Context Activation (NRSPCA) functionality:

• sgsn-nrspca-actv-rej-by-sgsn(515)
• sgsn-nrspca-actv-rej-by-ms(516)

The following new disconnect reason has been added in support of the new ISR functionality added in this release:

• sgsn-dbr-cause-isr-deact-detach(552)

show session subsystem facility aaaproxy all, show session subsystem facility aaaproxy data-info, show session subsystem facility aaaproxy debug-info

New statistics have been introduced to support LCS-MO-CDRs.

• Total LCS-MO-CDRs
• Current LCS-MO-CDRs

show sgsn fsm-statistics

The output of this command provides fields that track statistics for 3G SGSN (both Gn and S4) application finite state machine (FSM) statistics.

Table 2. show sgsn fsm-statistics Command Output Fields

<table>
<thead>
<tr>
<th>UMTS SMA FSM Statistics</th>
<th>Event</th>
<th>Hit Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMA_ST_PDP_Inactive</td>
<td>SMA_EVT_Actv_PDP_Ctxt_Req</td>
<td>:0</td>
</tr>
<tr>
<td>SMA_ST_PDP_Active</td>
<td>SMA_EVT_Release_Session_Req</td>
<td>:0</td>
</tr>
<tr>
<td>SMA_ST_Activate_Pending_Alloc_Res_Req</td>
<td>SMA_EVT_MS_Activate_New_Sess_Rej</td>
<td>:0</td>
</tr>
<tr>
<td>SMA_ST_Activate_Pending_Rab_Estab_Res</td>
<td>SMA_EVT_RAB_Assign_Resp_Success</td>
<td>:0</td>
</tr>
</tbody>
</table>
### SGSN Changes in Release 15.0

### SGSN Enhancements for September 30, 2013

---

<table>
<thead>
<tr>
<th>SMA_ST_Activate_Pending_Realloc_Res_Req</th>
<th>SMA_EVT_New_Session_Accept</th>
<th>0</th>
</tr>
</thead>
</table>

**UMTS Gn SMN FSM Statistics**

None

**UMTS S4 SMN FSM Statistics**

<table>
<thead>
<tr>
<th>State</th>
<th>Event</th>
<th>Hit Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>S4_SMN_ST_PDP_INACTIVE</td>
<td>S4_SMN_EVT_MS_ACTIVATE_ALLOC_RES_REQ</td>
<td>0</td>
</tr>
<tr>
<td>S4_SMN_ST_EPS_BEARER_ACTIVE</td>
<td>S4_SMN_EVT_DBR_IND</td>
<td>0</td>
</tr>
<tr>
<td>S4_SMN_ST_ACTIVATE_PENDING_SMGR_ANSWER_SESS</td>
<td>S4_SMN_EVT_ANSWER_SESSION</td>
<td>0</td>
</tr>
<tr>
<td>S4_SMN_ST_ACTIVATE_PENDING_CSR_RESP</td>
<td>S4_SMN_EVT_CSR_RESP_SUCCESS</td>
<td>0</td>
</tr>
<tr>
<td>S4_SMN_ST_ACTIVATE_PENDING_REALLOC_RES_REQ</td>
<td>S4_SMN_EVT_MS_ACTIVATE_FINISH</td>
<td>0</td>
</tr>
<tr>
<td>S4_SMN_ST_SEC_ACTIVATE_PENDING_CBR</td>
<td>S4_SMN_EVT_CBR_REJ</td>
<td>0</td>
</tr>
</tbody>
</table>

**UMTS PMM FSM Statistics**

<table>
<thead>
<tr>
<th>State</th>
<th>Event</th>
<th>Hit Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>PMM_ST_DETACHED</td>
<td>PMM_EVT_MS_NEW_CON_INDICATION</td>
<td>0</td>
</tr>
<tr>
<td>PMM_ST_AWAITING_VALID_PDU</td>
<td>PMM_EVT_MS_ATTACH_RECD</td>
<td>0</td>
</tr>
<tr>
<td>PMM_ST_MAP_GLU_CNF_PENDING</td>
<td>PMM_EVT_MAP_GLU_CFM</td>
<td>0</td>
</tr>
<tr>
<td>PMM_ST_MS_ATTACH_COMP_PENDING</td>
<td>PMM_EVT_MS_ATTACH_COMP</td>
<td>0</td>
</tr>
</tbody>
</table>

Total number of FSM matrix usage =

---

**show sgsn-mode**

New field indicates whether GPRS MOCN has been enabled with the `gprs-mocn` command.

- Multi Operator Core NW (MOCN)

**show sgtpc statistics**

The following counters are included in the `show sgtpc statistics` command output to support the NRSPCA feature.

---

**Table 3. NRSPCA SGTPC Statistics**

<table>
<thead>
<tr>
<th>NRSPCA SGTC Statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initiate PDP Context Activation Request</td>
</tr>
</tbody>
</table>
NRSPCA SGTC Statistics

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Total IPCA Req</td>
<td>Retrans IPCA Req</td>
</tr>
<tr>
<td>Initial IPCA Req</td>
<td></td>
</tr>
</tbody>
</table>

Initiate PDP Context Activation Response:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Accepted</td>
<td>Retrans IPCA Rsp</td>
</tr>
<tr>
<td>Initial IPCA Rsp</td>
<td></td>
</tr>
<tr>
<td>Total Denied</td>
<td>Retrans IPCA Rsp</td>
</tr>
<tr>
<td>Initial IPCA Rsp</td>
<td></td>
</tr>
</tbody>
</table>

Initiate PDP Context Activation Response Not Sent (verbose only)

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Linked PDP deact coll</td>
<td>Retrans IPCA Req bef MS rsp</td>
</tr>
</tbody>
</table>

Initiate PDP Context Activation Request Denied (verbose only)

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>IPCA Req Denied</td>
<td>Service Not Supported</td>
</tr>
<tr>
<td>No Resources Available</td>
<td></td>
</tr>
<tr>
<td>System Failure</td>
<td>Mandatory IE Incorrect</td>
</tr>
<tr>
<td>Mandatory IE Mis</td>
<td>Optional IE Incorrect</td>
</tr>
<tr>
<td>Invalid Message Format</td>
<td>Context not Found</td>
</tr>
<tr>
<td>Semantic Error in TFT</td>
<td>Syntactic Error in TFT</td>
</tr>
<tr>
<td>Semantic Error in Pkt Fltr</td>
<td>Syntactic Error in Pkt Fltr</td>
</tr>
<tr>
<td>MS Not GPRS Responding</td>
<td>MS Refuses</td>
</tr>
<tr>
<td>Invalid Correlation Id</td>
<td>PDP without TFT already Active</td>
</tr>
<tr>
<td>BCM Violation</td>
<td>MS GPRS Suspended</td>
</tr>
<tr>
<td>Unknown cause</td>
<td></td>
</tr>
</tbody>
</table>

**show sgsn-service all**

New statistics have been introduced to support LCS-MO-CDRs.

- Accounting cdr-types: lcs mo-cdr

**show subscribers gprs-only full**

This command provides information that indicates whether ISR is activated for 2G subscribers, provides the MME tunnel endpoint ID being used for the ISR-activated 2G subscriber, and the IP address of the MME associated with the ISR-activated 2G subscriber.

- ISR-Activated: (True or False)
- MME Ctrl Teid: (MME Control Tunnel Endpoint Identifier)
- MME IP Address: (IP address of MME)

**show subscriber gprs-only full all**

The show command **show subscriber sgsn-only full all** has been updated to include a display for “SSAF” and “Emm_combined_ue_waiting” flags.

- SSAF
- EMM Combined UE Waiting Flag
show subscriber sgsn-only full all

The show command **show subscriber sgsn-only full all** has been updated to include a display for “SSAF” and “Emm_combined_ue_waiting” flags.

- SSAF
- EMM Combined UE Waiting Flag

show subscribers [ gprs-only | sgsn-only ] full

The following field has been added to identify bearer control mode information, as MS only or MS/NW, that is included in the Create/Update PDP Context messages:

- Bearer Control Mode

Output for this show command has been modified to display the last known locational information for a GPRS or UMTS detached subscriber with the following new field:

- Last known Location (RAI): <variable> CGI / SAC : <variable>

A new parameter has been added to the output for each of these commands. This represents the latest Bearer Control Mode (BCM mode) information received from a GGSN in Create PDP Context Response or Update PDP Context Request/Response messages.

- Bearer Control Mode

show supplementary-service statistics

New show command **show supplementary-service statistics** has been added to display Supplementary Service Information. The following counters are added to display the same:

- SS Messages
- 3G-Register Rx
- Discarded
- 3G-Register Tx
- Location Notification
- Current Location
- Current/Last known Loc Type
- 3G-Facility Rx
- Discarded
- 3G-Facility Tx
- 3G-RLC-Rx
- Abort
- Return Result
- Verification Response
- Permission Denied
- Permission Granted
- Reject
- Decode Error
- 3G-RLC-Tx
- Abort
- 3G-LCS guard timer expiry

The following counters have been added to the command output to track deferred LCS requests:

**Table 4. Supplementary Service Statistics**

<table>
<thead>
<tr>
<th>SS Messages:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>3G-Register Rx</td>
<td>2G-Register Rx</td>
</tr>
<tr>
<td>Area Event Report</td>
<td>Area Event Report</td>
</tr>
<tr>
<td>MOLR</td>
<td>MOLR</td>
</tr>
<tr>
<td>3G-Register Tx</td>
<td>2G-Register Tx</td>
</tr>
<tr>
<td>Location Notification</td>
<td>Location Notification</td>
</tr>
<tr>
<td>Current Location</td>
<td>Current Location</td>
</tr>
<tr>
<td>Current/Last known location</td>
<td>Current/Last known location</td>
</tr>
<tr>
<td>Area Even Request</td>
<td>Area Even Request</td>
</tr>
<tr>
<td>Area Even Cancel</td>
<td>Area Even Cancel</td>
</tr>
<tr>
<td>Periodic Loc Request</td>
<td>Periodic Loc Request</td>
</tr>
<tr>
<td>Periodic Loc Cancel</td>
<td>Periodic Loc Cancel</td>
</tr>
<tr>
<td>Location Update</td>
<td>Location Update</td>
</tr>
<tr>
<td>3G-Facility Rx</td>
<td>2G-Facility Rx</td>
</tr>
<tr>
<td>MOLR</td>
<td>MOLR</td>
</tr>
<tr>
<td>3G-Facility Tx</td>
<td>2G-Facility Tx</td>
</tr>
<tr>
<td>Area Event Report</td>
<td>Area Event Report</td>
</tr>
<tr>
<td>3G-RLC Rx</td>
<td>2G-RLC Rx</td>
</tr>
<tr>
<td>Return Result</td>
<td>Return Result</td>
</tr>
<tr>
<td>Location Notification</td>
<td>Location Notification</td>
</tr>
<tr>
<td>Permission Denied</td>
<td>Permission Denied</td>
</tr>
<tr>
<td>Permission Granted</td>
<td>Permission Granted</td>
</tr>
<tr>
<td>Area Even Request</td>
<td>Area Even Request</td>
</tr>
<tr>
<td>Area Even Cancel</td>
<td>Area Even Cancel</td>
</tr>
<tr>
<td>Periodic Loc Request</td>
<td>Periodic Loc Request</td>
</tr>
</tbody>
</table>
**SS Messages:**

<table>
<thead>
<tr>
<th>SS Messages</th>
<th>SS Messages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Periodic Loc Cancel</td>
<td>Periodic Loc Cancel</td>
</tr>
<tr>
<td>Location Update</td>
<td>Location Update</td>
</tr>
<tr>
<td>Reject</td>
<td>Reject</td>
</tr>
<tr>
<td>Return Error</td>
<td>Return Error</td>
</tr>
<tr>
<td>Abort</td>
<td>Abort</td>
</tr>
<tr>
<td>3G-RLC Tx</td>
<td>2G-RLC Tx</td>
</tr>
<tr>
<td>Return Result</td>
<td>Return Result</td>
</tr>
<tr>
<td>MOLR</td>
<td>MOLR</td>
</tr>
<tr>
<td>Reject</td>
<td>Reject</td>
</tr>
<tr>
<td>Return Error</td>
<td>Return Error</td>
</tr>
<tr>
<td>3G-Decode Error</td>
<td>2G-Decode Error</td>
</tr>
<tr>
<td>3G Guard timer expiry</td>
<td>2G Guard timer expiry</td>
</tr>
</tbody>
</table>

**Modified SGSN Output Fields and Counters**

This section identifies modified SGSN show command output fields and counters available in release 15.0.

**show iups-service**

The output for this command has been modified with a new values for the Check CS/PS Co-ordination field:

- Enabled
- Enabled (Homer Only)
- Enabled (Roamer only)
- Disabled

The previously displayed value options were Continue and Reject

**Deprecated SGSN Output Fields and Counters**

This section identifies deprecated SGSN output fields and counters that are no longer supported in release 15.0.

**show gmm-sm statistics**

The following counters related to Supplementary Services are removed from the `show gmm-sm statistics` command:

- SS Messages
- Loc-Not-Inv
- Loc-Not-Ret-Res
- RLC-Tx
- RLC-Rx
Chapter 21
S-GW Changes in Release 15.0

This chapter identifies features and functionality added to, modified for, or deprecated from 15.0 S-GW software releases.

The following points to changes made in this document to correct omissions or technical errors made in the previously published Release Change Reference. In content for:

- March 30, 2013:
  - Corrections to keyword descriptions in CSCum65866 - cli required to control pgw fteid in relocation create session response,
S-GW Enhancements for February 27, 2015

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
- ADC Enhancements
- CF Enhancements
- ECS Enhancements
- Firewall Enhancements
- GTPP Enhancements
- Lawful Intercept Enhancements
- InTracer Enhancements
- MVG Enhancements
- NAT Enhancements
- SNMP MIB Enhancements
- System & Platform Enhancements

---

**CSCur53899 - instance 5 should be sent in UL IDFT rsp from s.sgw to s.mme**

*Applicable Products: S-GW*

**Feature Changes**

**Behavior Change Due to Fix for CSCur53899**

The fix implemented for CSCur53899 has resulted in a behavior change.

**Previous Behavior:** The Bearer Context IE included in Indirect Data Forwarding Tunnel Response from the Source SGW to the Source MME was not carrying Instances 4 and 5.
New Behavior: The Bearer Context IE in Indirect Data Forwarding Tunnel Response from the Source SGW to the Source MME will now contain both instances 4 and 5.

Important: As per 3GPP TS 29.274 V11.12.0, Table 7.2.19-2, Note 2, for UL data forwarding if the S-GW does not have enough information to decide which of the F-TEID instance from S1-U and S-GW to include in the message, it may include both of them. As a result, the S-GW will send both instances 4 and 5 in the Response Message.

Customer Impact: Indirect Data Forwarding Tunnel Response messages from the S-GW would carry both instances 4 and 5 from the Source S-GW to the Source MME. So, that MME supports the messages.
S-GW Enhancements for March 30, 2014

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
- ADC Enhancements
- CF Enhancements
- ECS Enhancements
- Firewall Enhancements
- GTPP Enhancements
- Lawful Intercept Enhancements
- InTracer Enhancements
- MVG Enhancements
- NAT Enhancements
- SNMP MIB Enhancements
- System & Platform Enhancements

---

**CSCum63316 - SGW responds with Man. IE incorrect sent by Target SGSN (HO Testing)**

**Applicable Products:** S-GW

**Feature Changes**

**Enhancement to Handling of IDFT Messages**

Previously, a Create Session Request with oi=0 during a handover was rejected if a dedicated bearer with an IE Bearer context to be removed was present. The software has been enhanced to address this potential scenario.
Previous Behavior: CSR with oi=0 during a handover was rejected if a dedicated bearer with IE Bearer context to be removed was present.

New Behavior: The Create Session Request with oi=0 during a handover is now accepted by the system.

CSCum65866 - cli required to control pgw fteid in relocation create session response.

Applicable Products: S-GW

Feature Changes

Control of P-GW FTEID in Relocation with S-GW Change

The S-GW software has been enhanced to support control of the P-GW Fully Qualified Tunnel Endpoint Identifier (FTEID) for relocation Create Session Response procedures with an S-GW change. For backward compatibility with earlier 3GPP release peer nodes requiring P-GW FTEID in the Create Session Response procedures, this configurable can be enabled.

Command Changes

pgw-fteid-in-relocation-cs-rsp

This new command in S-GW Service Configuration Mode enables the S-GW to send the P-GW FTEID in Create Session Response procedures where there is an S-GW relocation change. By default, this setting is disabled.

configure

    context context_name

    sgw-service sgw_srv-name

    pgw-fteid-in-relocation-cs-rsp

    no pgw-fteid-in-relocation-cs-rsp

end

Notes:

- pgw-fteid-in-relocation-cs-rsp enables the sending of the P-GW FTEID in Create Session Response procedures where there is an S-GW relocation change.

- no pgw-fteid-in-relocation-cs-rsp disables the sending of the P-GW FTEID in Create Session Response procedures where there is an S-GW relocation change.

Performance Indicator Changes

show sgw-service all
This command has been enhanced to indicate if the S-GW is configured to enable or disabled the sending of the P-GW FTEID in Create Session Response procedures where there is an S-GW change.

- PGW Ctrl FTEID in Relocation Create Session Response: Disabled
- PGW Ctrl FTEID in Relocation Create Session Response: Enabled

**show configuration**

This command has been enhanced to indicate if the S-GW is configured to enable or disabled the sending of the P-GW FTEID in Create Session Response procedures where there is an S-GW change.

- pgw_fteid_in_relocation_cs_rsp

**CSCum97952 - Asrt @ fnc: sessmgr_sgw_gtp_pp_sess_acct_acct_cb**

*Applicable Products:* S-GW

**Feature Changes**

**Enhancement to Handling of IDFT Messages**

Certain scenarios were creating an Assert during messaging for the Indirect Data Forwarding Tunnel feature.

**Previous Behavior:** The Create indirect Data forwarding tunnel Request message was accepted for a bearer even if the Bearer was in one of the following states:

- Delete Bearer Pending
- Delete Bearer command pending
- Delete Session Request

As a result, even if the bearer was being deleted due to any one of the message listed below then the system also accepted the IDFT message.

- Delete Bearer message is in process and sent to the MME/SGSN
- Delete Session Request message is sent to the PGW
- Delete Bearer command is pending for the bearer

**New Behavior:** If any bearer is getting deleted then the system does not create an Indirect Data Forwarding Tunnel for the bearer. If all the bearers in the request are getting delete the reject complete request message is sent. If for some of the bearers the request will be accepted then the system processes the create Indirect Data Forwarding Request message.
S-GW Enhancements for November 30, 2013

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
- ADC Enhancements
- CF Enhancements
- ECS Enhancements
- Firewall Enhancements
- GTPP Enhancements
- Lawful Intercept Enhancements
- InTracer Enhancements
- MVG Enhancements
- NAT Enhancements
- SNMP MIB Enhancements
- System & Platform Enhancements

---

**CSCui75767 - SGW full checkpoint to micro checkpoint conversion - Phase 1**

**Feature Changes**

**S-GW Full Checkpoint to Micro Checkpoint Conversion**

To improve ICSR performance, S-GW can now send micro checkpoints instead of full checkpoints for several events to the standby chassis. This activity has been divided into 3 phases. The first phase includes optimizing checkpoints for the following events:

- UE active to idle transition
- UE idle to active transition (service request for all bearers)
- AMBR Change
- Bearer QoS Change
- Inter enodeb X2 HO
- MME to SGSN HO
- MME to SGSN TAU HO
- SGSN to MME HO
- SGSN to MME TAU HO
- Bearer Creation
S-GW Enhancements for September 30, 2013

S-GW Feature Changes as of September 30, 2013

This section provides information on S-GW feature changes in release 15.0.

**Important:** For more information regarding features in this section, refer to the *S-GW Administration Guide* for this release.

New S-GW Features

This section identifies new S-GW features available in release 15.0.

Intelligent Paging for ISR

**Important:** This feature has been implemented as lab quality. All associated CLI commands and performance statistics are also now supported at lab quality.

**Important:** Use of Intelligent Paging for ISR in S-GW requires that a valid license key be installed. Contact your Cisco account representative for information on how to obtain a license.

In case of Idle-mode Signaling Reduction (ISR) active and UE is idle, the S-GW will send Downlink Data Notification (DDN) Message to both the MME and the S4-SGSN if it receives the downlink data or network initiated control message for this UE. In turn, the MME and the S4-SGSN would do paging in parallel consuming radio resources.

To optimize the radio resource, the S-GW will now perform intelligent paging. When configured at S-GW service level for each APN, the S-GW will page in a semi-sequential fashion (one by one to peer MME or S4-SGSN based on last known RAT type) or parallel to both the MME and S4-SGSN.

If the S-GW receives Data packet on a bearer for a UE in IDLE state and the S-GW is configured to initiate semi-sequential paging for that APN then following is will be done:

- The S-GW receives the downlink data packet for an ISR active and Idle UE.
- The S-GW is configured to initiate semi-sequential paging for this APN and last known RAT Type for this UE is EUTRAN.
- The S-GW initiates Downlink Data Notification (DDN) towards MME and starts the timer \( t_p \).
- If the MME initiates the service request procedure for this UE within time ‘\( t_p \)’ then the S-GW will stop the timer \( t_p \) and process the service request procedure and will not initiate the DDN towards S4-SGSN (another RAT). This avoids the unnecessary paging attempt and use of radio resources.
- If the MME does not initiates the service request procedure for this UE within time \( t_p \) then after expiry of timer \( t_p \), the S-GW will initiate the DDN towards S4-SGSN.

Similar behavior is followed if the last known RAT is UTRAN/GERAN. Initially the S-GW will send DDN only to S4-SGSN.
LIPA Support

A LIPA (Local IP Access) PDN is a PDN Connection for local IP access for a UE connected to a HeNB. The LIPA architecture includes a Local Gateway (LGW) acting as an S-GW GTPv2 peer. The LGW is collocated with HeNB in the operator network behaves as a PGW from SGW perspective. Once the default bearer for the LIPA PDN is established, then data flows directly to the LGW and from there into the local network without traversing the core network of the network operator.

In order to support millions of LIPA GTPC peers, S-GW memory management has been enhanced with regards to GTPv2 procedures and as well as to support the maintenance of statistics per peer node.

Establishment of LIPA PDN follows a normal call flow similar to that of a normal PDN as per 23.401; the specification does not distinguish between a LGW and a PGW call. As a result, the S-GW supports a new configuration option to detect a LIPA peer. As a fallback mechanism, heuristic detection of LIPA peer based on data flow characteristics of a LIPA call is also supported.

Whenever a peer is detected as a LIPA peer, the S-GW will disable GTPC echo mechanism towards that particular peer and stop maintaining some statistics for that peer.

A configuration option in APN profile explicitly indicates that all the PDN’s for that APN are LIPA PDN’s, so all GTPC peers on S5 for that APN are treated as LGW, and thus no any detection algorithm is applied to detect LGW.

Node Functionality GTP Echo

This feature helps exchange capabilities of two communicating GTP nodes, and uses the new feature based on whether it is supported by the other node.

This feature allows S-GW to exchange its capabilities (MABR, P-GW Restart Notification, NTSR) with the peer entities through ECHO messages. By this, if both the peer nodes support some common features, then they can make use of new messages to communicate with each other.

With new “node features” IE support in ECHO request/response message, each node can send its supported features (MABR, P-GW Restart Notification, NTSR). This way, S-GW can learn the peer node’s supported features. S-GW’s supported features can be configured by having some configuration at the service level.

If S-GW wants to use new message, such as P-GW Restart Notification, then S-GW should check if the peer node supports this new feature or not. If the peer does not support it, then S-GW should fall back to old behavior.

If S-GW receives a new message from the peer node, and if S-GW does not support this new message, then S-GW should ignore it. If S-GW supports the particular feature, then it should handle the new message as per the specification.

Overcharging Protection Support

Overcharging Protection helps in avoiding charging the subscribers for dropped downlink packets while the UE is in idle mode. In some countries, it is a regulatory requirement to avoid such overcharging, so it becomes a mandatory feature for operators in such countries. Overall, this feature helps ensure subscriber are not overcharged while the subscriber is in idle mode.

**Important:** Use of Overcharging Protection in S-GW requires that a valid license key be installed. Contact your Cisco account representative for information on how to obtain a license.

P-GW will never be aware of UE state (idle or connected mode). Charging for downlink data is applicable at P-GW, even when UE is in idle mode. Downlink data for UE may be dropped at S-GW when UE is in idle mode due to buffer overflow or delay in paging. Thus, P-GW will charge the subscriber for the dropped packets, which isn’t desired. To address this problem, with Overcharging Protection feature enabled, S-GW will inform P-GW to stop or resume charging based on packets dropped at S-GW and transition of UE from idle to active state.
Once the criterion to signal “stop charging” is met, S-GW will send Modify Bearer Request (MBReq) to P-GW. MBReq would be sent for the PDN to specify which packets will be dropped at S-GW. MBReq will have a new private extension IE to send “stop charging” and “start charging” indication to P-GW.

When the MBReq with stop charging is received from a S-GW for a PDN, P-GW will stop charging for downlink packets but will continue sending the packets to S-GW.

P-GW will resume sending downlink packets after receiving “stop charging” request when either of these conditions is met:

- When the S-GW (which had earlier sent “stop charging” in MBReq) sends “start charging” in MBReq.
- When the S-GW changes (which indicates that maybe UE has relocated to new S-GW).

**Peer GTP Node Profile Configuration Support**

Provides flexibility to the operators to have different configuration for GTP-C and Lawful Intercept, based on the type of peer or the IP address of the peer.

Peer profile feature allows flexible profile based configuration to accommodate growing requirements of customizable parameters with default values and actions for peer nodes of S-GW. With this feature, configuration of GTP-C parameters and disabling/enabling of Lawful Intercept per MCC/MNC or IP address based on rules defined.

A new framework of peer-profile and peer-map is introduced. Peer-profile configuration captures the GTP-C specific configuration and/or Lawful Intercept enable/disable configuration. GTP-C configuration covers GTP-C retransmission (maximum number of retries and retransmission timeout) and GTP echo configuration. Peer-map configuration matches the peer-profile to be applied to a particular criteria. Peer-map supports criteria like MCC/MNC (PLMN-ID) of the peer or IP-address of the peer. Peer-map can then be associated with S-GW service.

Intent of this feature is to provide flexibility to operators to configure a profile which can be applied to a specific set of peers. For example, have a different retransmission timeout for foreign peers as compared to home peers.

**P-GW Restart Notification Support**

This procedure optimizes the amount of signaling involved on S11/S4 interface when P-GW failure is detected.

P-GW Restart Notification Procedure is a standards-based procedure supported on S-GW to notify detection of P-GW failure to MME/S4-SGSN. P-GW failure detection will be done at S-GW when it detects that the P-GW has restarted (based on restart counter received from the restarted P-GW) or when it detects that P-GW has failed but not restarted (based on path failure detection). When an S-GW detects that a peer P-GW has restarted, it shall locally delete all PDN connection table data and bearer contexts associated with the failed P-GW and notify the MME via P-GW Restart Notification. S-GW will indicate in the echo request/response on S11/S4 interface that the P-GW Restart Notification procedure is supported.

P-GW Restart Notification Procedure is an optional procedure and is invoked only if both the peers, MME/S4-SGSN and S-GW, support it. This procedure optimizes the amount of signaling involved on S11/S4 interface when P-GW failure is detected. In the absence of this procedure, S-GW will initiate the Delete procedure to clean up all the PDNs anchored at that failed P-GW, which can lead to flooding of GTP messages on S11/S4 if there are multiple PDNs using that S-GW and P-GW.

**Modified S-GW Features**

This section identifies S-GW features modified in release 15.0.

**3GPP TS 29.274 Release 10 Compliance**

The following changes have been introduced for compliance with 3GPP TS 29.274 Release 10.
CR-698: Notification of supported features between peer GTP-C entities
A node shall signal to a direct peer node the list of features it supports by sending the Sending Node Features IE in the Echo Request and Echo Response messages. Refer to the Node Functionality GTP Echo section under New S-GW Features for more information.

CR-783: ISR in the Detach procedure
- **Previous Behavior:** When DSReq is received with oi=0 from both the MME and S4-SGSN in Idle-mode Signaling Reduction (ISR) case, the S-GW did not forward DSReq to the P-GW.
- **New Behavior:** When DSReq is received from both the MME and S4-SGSN with oi=0 in ISR case, the S-GW will now forward the DSReq to the P-GW.

CR-816: Essential alignment with PMIP spec
The modification for CR-816 is supported.

CR-867: Correcting IE Type for Bearer QoS IE from Variable to Extendable
The Bearer QoS IE is corrected as an “Extendable” type IE, as per table 8.1-1.

CR-885: Essential correction to the to GTPv2 cause table
The modification for CR-885 is supported.

CR-887: Unsupported bearer handling for LIPA
If a Bearer Resource Command message is related to an established PDN connection for Local IP Address (LIPA), the Local-GW (LGW) shall reject the Bearer Resource Command with the new EGTP cause value of “Bearer handling not supported”.

CR-911: Inclusion of Node Type in DDN Failure Indication when the ISR is active
EGTPC is modified to update the peer type based on the 'Originating Node' IE received in DDN failure indication message.

CR-944: Max MBR/APN-AMBR
The S-GW now supports sending the new IE “Max APN-AMBR” received in Create Session Request or Modify Bearer Request messages. The EGTPC module provides the support to encode, decode and validate the IE and forward the message to the P-GW.

CR-982: IP address parameter
- **Previous Behavior:** After inter-S-GW HO, the S-GW could not set the dynamic address flag correctly in the SGW-CDR because the P-GW was not sending this info to the S-GW in MBR message.
- **New Behavior:** The static address flag is sent from the P-GW in the TAU/RAU/Handover with S-GW change procedure. The S-GW can now send the correct value of dynamic address flag in the SGW-CDR.

CR-1021: Essential clarification on F-TEID in Create Bearer Response
- **Previous Behavior:** In CBReq, if S-GW is sending S4-U FTEID, in response it was expecting only S4-U FTEID in CBRsp. Otherwise the CBReq is getting rejected. Same behavior was used for S12 FTEID.
- **New Behavior:** Irrespective of F-TEID sent in CBReq (S4-U or S12), the S-GW accepts CBRsp with either S4-U or S12 FTEID.

CR-1052: Defining the fixed number of octets for extendable IEs
For each Fixed and Extendable IE, “Fixed number of Octets” are explicitly defined. The receiving node should only expect “Fixed number of Octets” for the extendable IEs.
CR-1057: Essential correction to the TAD IE inclusion in Bearer Resource Command over S4

- **Previous Behavior:** Since TAD IE is mandatory in Bearer Resource Command, EGTPC rejects the Bearer Resource Command if the TAD IE is missing.

- **New Behavior:** For S4-SGSN, TAD IE marked as conditional over S4 interface. If S4-SGSN receives this IE from the UE, it shall include it over S4 interface. So at EGTPC, message validation is changed for the presence of this IE. If S-GW receives this IE, the S-GW will forward it to P-GW over S5/S8 interface.

CR-1095: Correction on the bearer context for mod procedure

- **Previous Behavior:** It was unclear whether or not to include the Bearer context to be modified IE in the MBR message over the S5/S8 interfaces for a TAU/RAU/HO without S-GW change procedure.

- **New Behavior:** The bearer context to be modified IE is not included in the MBR message over the S5/S8 interfaces for a TAU/RAU/HO without S-GW change procedure.

CR-1102: Missing Cause Value for MUPSAP

- **Previous Behavior:** There was no specific rejection cause defined for Create Session Request for additional PDN connectivity request in PMIP bases S5/S8 scenario, even though it was not allowed.

- **New Behavior:** New rejection cause “Multiple PDN connections for a given APN not allowed” is defined for S-GW in the reply message for Create Session Request for additional PDN connectivity to the MME/S4-SGSN when PMIP-based S5/S8 is used.

CR-1105: Downlink bearers release during mobility

- **Previous Behavior:** In the TAU/RAU without S-GW change procedure, the target MME/SGSN sends the Modify Bearer Request message to the S-GW. No downlink userplane information is included in this message. As the source SGSN may not remove the SGSN IP address and TEID in the S-GW when the UE comes to IDLE state, or the UE may be in ECM-CONNECTED state in the source side, if the S-GW maintains the connection with the source side, userplane data will be sent to the source network.

- **New Behavior:** Bearer Context To be Modified IE will be included in the above Modify Bearer Request message with the mandatory EBI IE. If only EBI is included, the S-GW will remove the downlink userplane information.

### 3GPP TS 29.281 (GTP-U) Release 10 Compliance

**Previous Behavior:** S-GW was not fully compliant to 3GPP TS 29.281 Rel-10 to support UDP Port Extension header in Error indication message and Supported Extension Headers Notification message.

**New Behavior:** This feature enhances the GTP-U capabilities of S-GW in compliance to 3GPP TS 29.281 Release 10. Support for UDP Port Extension Header in Error Indication message and Supported Extension Headers Notification message was added to become fully compliant with 3GPP Release 10.

Supported Extension Headers Notification message indicates a list of supported extension headers that the node can support. This message is sent only in case a GTP entity was required to interpret a mandatory extension header (by setting the comprehension required in extension header), but the GTP entity was not yet upgraded to support that extension header.

- If a Supported Extension Headers Notification is received from peer GTP-U entity, node will not send the extension header to the peer entity.

- If a message which contains extension header is received from peer GTP-U entity and the extension header is set to comprehension required and the extension header cannot be interpreted by the node, it will send a Supported Extension Headers Notification message. This message shall include all the extension headers supported by the node.
UDP Port Extension header helps in handling the Error-Indication message efficiently. If any GTP-U peer supports this extension header, then sending this extension header in Error-Indication message will help in processing the Error-Indication message.

Support for Supported Extension Headers Notification message helps notify the GTP-U peer about the GT-U capabilities of the node. This message is sent only in case the node was required to interpret a mandatory extension header (by setting the comprehension required in extension header), but the node was not yet upgraded to support that extension header.

**Bearer Context to be Modified IE in MBR Message**

The Modify Bearer Request message can be triggered by the UE time zone, ULI and/or RAT Type in the TAU/RAU/Handover without S-GW change procedure. In these procedures, there is no need to include the Bearer Context to be Modified IE.

**Previous Behavior:** The S-GW included the MBR message without change procedure.

**New Behavior:** The Bearer Context to be Modified IE is not included in the MBR message over the S5/S8 interfaces for a TAU/RAU/HO without S-GW change procedure.

**Create Indirect Data Forwarding Tunnel Response Change**

The Create Indirect Data Forwarding Tunnel Response message can now have cause value set to “Request accepted partially”.

**EPS Bearer ID and ARP Support in DDN**

This feature allows support for Priority Paging support in the network. This is mainly needed for MPS subscriber support. The paging priority in the paging message is set by MME based on ARP received in Downlink Data Notification message.

In order to support MPS requirement for Priority Paging in the network for MPS subscriber, DDN message has been enhanced to support passing ARP and EBI information. When the S-GW sends a Downlink Data Notification message, it shall include both EPS Bearer ID and ARP. If the Downlink Data Notification is triggered by the arrival of downlink data packets at the S-GW, the S-GW shall include the EPS Bearer ID and ARP associated with the bearer on which the downlink data packet was received. If the Downlink Data Notification is triggered by the arrival of control signaling, the S-GW shall include the EPS Bearer ID and ARP, if present in the control signaling. If the ARP is not present in the control signaling, the S-GW shall include the ARP in the stored EPS bearer context. If multiple EPS Bearers IDs are reported in the Downlink Data Notification message, the S-GW shall include all the EBI values and the ARP associated with the bearer with the highest priority (lowest ARP value). For more information, see TS 23.401 (section 5.3.4.3) and 29.274 (section 7.2.11). Details are discussed in CR-859 of 3GPP specifications.

**GTPv2 Cause IMSI Not Known Changed to IMSI/IMEI Not Known**

When the UE is UICC-less and emergency attached, there is no valid IMSI. So it is not possible to provide the IMSI in the related messages like Change Notification Requests. In this case, the IMEI is included in these messages. If the IMEI is not known in the target side, the correct cause should be returned to the source side.

**Previous Behavior:** GTPv2 cause was previously 'IMSI not known'

**New Behavior:** The cause “IMSI not known” is changed to “IMSI/IMEI not known” and changed in the related response messages.

**Higher Bitrates Than 16 Mbps Flag**
The Higher bitrates than 16 Mbps flag is added into GTPv2 IE MM Context. Since the Higher bitrates than 16 Mbps flag is only concerning Pre-release 7 UMTS UE, this flag shall be only added into “UMTS Key, Used Cipher and Quintuplets”, “GSM Key, Used Cipher and Quintuplets”, “UMTS Key and Quintuplets”.

**Indirect Forward Tunneling - DL and UL Forwarding**

Support is provided for LTE to 3G PS Handovers with downlink and uplink indirect data forwarding in this release.

**Management Based MDT Allowed Flag**

The Management Based MDT (Minimization of Drive Tests) Allowed flag is added to Indication IE in Forward Relocation Request and the Context Response messages, and to the definition of the Indication IE.

**New Rejection Cause for MUPSAP**

In PMIP-based S5/S8 scenarios, when the S-GW receives a Create Session Request for additional PDN connectivity request, the S-GW responds to the request with a rejection cause if either the S-GW or P-GW does not support multiple PDN connections to the same APN (MUPSAP).

**Previous Behavior:** There was no specific rejection cause for this scenario.

**New Behavior:** A new rejection cause “Multiple PDN connections for a given APN not allowed” is defined for S-GW in the reply message to the MME/S4-SGSN when PMIP-based S5/S8 is used.

**S-GW Command Changes as of September 30, 2013**

This section provides information on S-GW command changes in release 15.0.

### Important:
For more information regarding commands in this section, refer to the Command Line Interface Reference for this release.

**New S-GW Commands**

This section identifies new S-GW commands available in release 15.0.

**description**

The following new command configures a short description for the specified peer profile.

```
configure

peer-profile service-type sgw-network { default | name profile_name } [ -noconfirm ]

description description

no description

end
```

**egtp**
Configuration related to handling eGTP procedure.

```
cfg
    sgw-service service_name [ -noconfirm ] [ default ] egtp cause-code temp-failure db-proc
    no egtp cause-code temp-failure
end
```

Note:

- `cause-code temp-failure db-proc`: Enables handling of Delete Bearer failure response from peer with cause code 110 (Temporary Failure).
- Default behavior is Disabled.

**gtpc**

The following new command configures the GTP-C settings for the specified peer profile.

```
cfg
    peer-profile service-type sgw-network { default | name profile_name } [ -noconfirm ]
    gtpc { echo { interval seconds | retransmission-timeout seconds } | max-retransmissions seconds | retransmission-timeout seconds }
    default gtpc { echo { interval | retransmission-timeout } | max-retransmissions | retransmission-timeout }
    no gtpc echo
end
```

Notes:

- `gtpc echo interval seconds` must be an integer from 60 to 3600. Default: 60
- `gtpc echo retransmission-timeout seconds` must be an integer from 1 to 20. Default: 5
- `gtpc max-retransmissions number` must be an integer from 0 to 15. Default: 4
- `gtpc retransmission-timeout seconds` must be an integer from 1 to 20. Default: 5

**isr-sequential-paging**

Initiates Intelligent Paging for ISR feature for specified APN Profile, where paging first towards the last known RAT, then towards the other RAT.

```
cfg
```
apn-profile profile_name [ -noconfirm ]
[ remove ] isr-sequential-paging
end

**Important:** Intelligent Paging for ISR functionality has been implemented as lab quality.

**lgw-detection**

Enables Local Gateway (LGW) detection. LIPA architecture includes an LGW acting as an S-GW GTPv2 peer.

```configure
sgw-service service_name [ -noconfirm ]
lgw-detection [ window-time minutes threshold-count lipa_pdns
   no lgw-detection
end
```

**Note:**
- **window-time:** Configures polling window for LGW detection algorithm.
  `minutes` must be an integer from 5 to 250.
- **threshold-count:** Configures threshold count for LGW detection algorithm.
  `lipa_pdns`: The number of LIPA PDNs that should pattern match before peer is marked as LGW. Must be an integer from 1 to 999999999.

**lipa-apn**

S-GW identifies an APN as LIPA (Local IP Access) APN.

```configure
apn-profile profile_name [ -noconfirm ]
lipa-apn
end
```

**msisdn**

Certain digits from the MSISDN will be used with the APN DNS Query String.

```configure
apn-profile profile_name [ -noconfirm ]
msisdn <string_1-15>
end```
multi-access

APN is configured as multi access and there will be two different sessions at P-GW for different access tech.

```
configure

    apn-profile profile_name [ -noconfirm ]

    multi-access

end
```

overcharge-protection

Enables overcharge protection for APNs controlled by this APN profile. Each overcharging protection option is a standalone configuration and it doesn't override the previous option set, if any.

```
configure

    apn-profile profile_name [ -noconfirm ]

    [ remove ] overcharge-protection { abnormal-s1-release | ddn-failure | drop-limit
        number { packets | bytes } }

end
```

Notes:

- **drop-limit number**: Send MBR to pause charging at P-GW if specified number of packets/bytes is dropped for a PDN connection.
- **abnormal-s1-release**: (for future use) if overcharging protection is enabled for abnormal-s1-release, S-GW would send MBR to pause charging at P-GW if it Abnormal Release of Radio Link signal from MME. (Though the command is present, in this release this scenario is not possible).
- **ddn-failure**: if overcharging protection is enabled for ddn-failure message, MBR would be sent to P-GW to pause charging upon receiving DDN failure from MME/S4-SGSN.

**Important**: Overcharge Protection functionality has been implemented as lab quality.

peer-map

The following new command creates a peer map and enters the Peer Map Configuration mode. This new command mode enables the operator to map and LTE Policy to a peer profile based on matching criteria and precedence for the criteria.

```
configure

    lte-policy

    peer-map map_name [ -noconfirm ]

    no peer-map map_name

end
```
peer-profile

The following command creates an S-GW network peer profile and enters the Peer Profile Configuration mode.

configure

peer-profile service-type sgw-network { default | name profile_name } [ -noconfirm ]

no peer-profile service-type sgw-network name profile_name

end

Note:
• A maximum of 64 peer profiles can be configured.

precedence

The following new command configures the matching criteria and precedence for mapping an LTE Policy with a peer profile.

configure

lte-policy

peer-map map_name [ -noconfirm ]

precedence priority match-criteria { all peer-profile-name profile_name | peer-ip-address { ip_address | ip_address/mask } | serving-plmnid mcc mcc mcc | peer-profile-name profile_name | serving-plmnid mcc mcc mcc | peer-ip-address { ip_address | ip_address/mask } | peer-profile-name profile_name }

no precedence priority

end

Notes:
• Precedence 1 has highest priority.
  priority must be an integer from 1 to 1024.
• A maximum of 1024 precedence entries can be configured.
• To map a peer to a profile when there is no specific criteria required, use the all keyword.
• mcc must be a three-digit number between 100 and 999.
• mnc must be a two- or three-digit number between 00 and 999.

show peer-profile

The following command displays configuration of the specified peer profile.

show peer-profile { all | full { all | name profile_name } | name profile_name }
Modified S-GW Commands

This section identifies S-GW commands modified in release 15.0.

associate

The new keyword **peer-map** associates an LTE Policy peer map with an S-GW service.

```
configure
  context context_name
  sgw-service svc_name
    associate peer-map map_name
    no associate peer-map
  end
```

ddn isr-sequential-paging delay-time

This command includes a new **delay-time** keyword to configure the delay time in 100 millisecond increments between paging of different RAT types in support of the Intelligent Paging for ISR feature.

```
configure
  context context_name
  sgw-service svc_name
    ddn isr-sequential-paging delay-time delay
    default ddn isr-sequential-paging
  end
```

Notes:
- **delay** must be an integer from 1 to 255, representing increments of 100 milliseconds (**delay** = 1-255 * 100 ms).
- Default: 10 (10 * 100 ms = 1 second)

> **Important:** Intelligent Paging for ISR functionality has been implemented as lab quality.

gtpc

This command has been modified to enable P-GW Restart Notification functionality.

```
configure
  context <context_name>
    egtp-service <svc_name>
```
gtpp node-feature pgw-restart-notification svc_name
end

plmn id

In previous releases, a maximum of 5 PLMN IDs could be configured. In this release, up to 15 PLMN IDs can be configured per S-GW service.

configure

  context context_name

    sgw-service svc_name

    plmn id mcc number mnc number [ primary ]

  end

show lte-policy peer-map

The new keyword peer-map displays configuration of the specified LTE Policy peer map.

show lte-policy peer-map { name map_name | summary }

Deprecated S-GW Commands

This section identifies deprecated S-GW commands that are no longer supported in release 15.0.
None for this release.

S-GW Performance Indicator Changes as of September 30, 2013

This section provides information on S-GW performance indicator changes in release 15.0.

Important: For more information regarding bulk statistics and output fields and counters in this section, refer to the Statistics and Counters Reference for this release.

New S-GW Bulk Statistics

This section identifies new S-GW bulk statistics available in release 15.0.

New in the eGTP-C Schema

The following bulkstats have been added:

- tun-recv-cresessNorsp
- tun-recv-cresessDiscard

The following bulkstats have been added for Create Session Response:
[S-GW Enhancements for September 30, 2013]

- tun-sent-cresessrespdeniedCtxtNotFound
- tun-sent-cresessrespdeniedInvalidMsgFormat
- tun-sent-cresessrespdeniedInvalidLength
- tun-sent-cresessrespdeniedMandIEIncorrect
- tun-sent-cresessrespdeniedMandIEMissing
- tun-sent-cresessrespdeniedNoResourcesAvl
- tun-sent-cresessrespdeniedMissingUnknownApn
- tun-sent-cresessrespdeniedPrefPdnTypeUnsupported
- tun-sent-cresessrespdeniedAllDynamicAddrOccupied
- tun-sent-cresessrespdeniedServiceDenied
- tun-sent-cresessrespdeniedUserAuthFailed
- tun-sent-cresessrespdeniedApnAccessDenied
- tun-sent-cresessrespdeniedRequestRejected
- tun-sent-cresessrespdeniedCondIEMissing
- tun-sent-cresessrespdeniedApnRstTypeIncompatible
- tun-sent-cresessrespdeniedImsiNotKnown
- tun-sent-cresessrespdeniedOtherCause

The following bulkstats have been added:

- tun-recv-cresessrespDiscard
- tun-recv-crebearDiscard
- tun-recv-crebearNorsp
- tun-recv-crebearrespDiscard

The following bulkstats have been added for Create Bearer Response:

- tun-recv-crebearrespdeniedCtxtNotFound
- tun-recv-crebearrespdeniedSvcNotSupported
- tun-recv-crebearrespdeniedInvalidMsgFormat
- tun-recv-crebearrespdeniedMandIEIncorrect
- tun-recv-crebearrespdeniedMandIEMissing
- tun-recv-crebearrespdeniedCondIEMissing
- tun-recv-crebearrespdeniedNoResourcesAvl
- tun-recv-crebearrespdeniedSemanticErrinTFT
- tun-recv-crebearrespdeniedSyntacticErrinTFT
- tun-recv-crebearrespdeniedSemanticErrinPktFltr
- tun-recv-crebearrespdeniedSyntacticErrinPktFltr
- tun-recc-crebearrespdeniedUnableToPageUE
- tun-recc-crebearrespdeniedUENotResponding
- tun-recc-crebearrespdeniedUnableToPageUeSuspend
- tun-recc-crebearrespdeniedUERefuses
- tun-recc-crebearrespdeniedRequestRejected
- tun-recc-crebearrespdeniedInvalidLenPiggybkMsg
- tun-recc-crebearrespdeniedInvalidRemotePeerReply
- tun-recc-crebearrespdeniedPeerNotResponding
- tun-recc-crebearrespdeniedTempRejDueToHOProgress
- tun-recc-crebearrespdeniedDeniedInRat
- tun-recc-crebearrespdeniedOtherCause

The following bulkstats have been added:

- tun-recc-bearrescmdDiscard
- tun-recc-bearrescmdNorsp
- tun-recc-bearrescmd-failDiscard
- tun-recc-modbearreqDiscard
- tun-recc-modbearreqNorsp
- tun-recc-modbearrespDiscard
- tun-recc-delsessreqDiscard
- tun-recc-delsessreqNorsp

The following bulkstats have been added for Delete Session Response:

- tun-sent-delsessrespdeniedCtxtNotFound
- tun-sent-delsessrespdeniedInvalidMsgFormat
- tun-sent-delsessrespdeniedMandIEIncorrect
- tun-sent-delsessrespdeniedMandIEMissing
- tun-sent-delsessrespdeniedNoResourcesAvl
- tun-sent-delsessrespdeniedOtherCause

The following bulkstats have been added:

- tun-recv-delsessrespDiscard
- tun-recv-delbearreqDiscard
- tun-recv-delbearreqNorsp
- tun-recv-delbearrespDiscard

The following bulkstats have been added for Delete Bearer Response:

- tun-recv-delbearrespdeniedCtxtNotFound
- tun-recev-delbearrespdeniedInvalidMsgFormat
- tun-recev-delbearrespdeniedMandIEIncorrect
- tun-recev-delbearrespdeniedMandIEMissing
- tun-recev-delbearrespdeniedCondIEMissing
- tun-recev-delbearrespdeniedNoResourcesAvl
- tun-recev-delbearrespdeniedRequestRejected
- tun-recev-delbearrespdeniedUnableToPageUeSuspend
- tun-recev-delbearrespdeniedInvalidRemotePeerReply
- tun-recev-delbearrespdeniedPeerNotResponding
- tun-recev-delbearrespdeniedTempRejDueToHOProgress
- tun-recev-delbearrespdeniedOther

The following bulkstats have been added:

- tun-recev-dlinknotifDiscard
- tun-recev-dlinknotifNorsp
- tun-recev-dlinknotifackDiscard
- tun-recev-dlinkdatafailDiscard
- tun-recev-relacebearreqDiscard
- tun-recev-relacebearreqNorsp
- tun-recev-relacebearrespDiscard
- tun-recev-modbearcmdDiscard
- tun-recev-modbearcmdNorsp
- tun-recev-modbearfailDiscard
- tun-recev-delbearcmdDiscard
- tun-recev-delbearcmdNorsp
- tun-recev-delbearfailDiscard
- tun-recev-updbearreqDiscard
- tun-recev-updbearreqNorsp
- tun-recev-updbearrespDiscard

The following bulkstats have been added for Update Bearer Response:

- tun-recev-updbearrespdeniedCtxtNotFound
- tun-recev-updbearrespdeniedInvalidMsgFormat
- tun-recev-updbearrespdeniedMandIEIncorrect
- tun-recev-updbearrespdeniedMandIEMissing
- tun-recev-updbearrespdeniedNoResourcesAvl
- tun-recev-updbearspdeniedSemanticErrInTFT
- tun-recev-updbearspdeniedSyntacticErrInTFT
- tun-recev-updbearspdeniedSemanticErrInPktFltr
- tun-recev-updbearspdeniedSyntacticErrInPktFltr
- tun-recev-updbearspdeniedUENotResponding
- tun-recev-updbearspdeniedUERefuses
- tun-recev-updbearspdeniedUnableToPageUE
- tun-recev-updbearspdeniedRequestRejected
- tun-recev-updbearspdeniedUnableToPageUeSuspend
- tun-recev-updbearspdeniedCondIEMissing
- tun-recev-updbearspdeniedInvalidRemotePeerReply
- tun-recev-updbearspdeniedPeerNotResponding
- tun-recev-updbearspdeniedTempRejDueToHOProgress
- tun-recev-updbearspdeniedOtherCause

The following bulkstats have been added:

- tun-recev-creinddatafwdngreqDiscard
- tun-recev-creinddatafwdngreqNorsp
- tun-recev-creinddatafwdngrspDiscard
- tun-recev-delinddatafwdngreqDiscard
- tun-recev-delinddatafwdngrspDiscard
- tun-recev-changenotfreqDiscard
- tun-recev-changenotfreqNorsp
- tun-recev-changenotfrespDiscard

The following bulkstats have been added for P-GW Restart Notification support:

- tun-sent-pgwRstnotfreq
- tun-sent-retranspgwRstnotfreq
- tun-sent-noRspPgwRstnotfreq
- tun-recev-pgwRstnotfackp
- tun-recev-pgwRstnotfackpaccept
- tun-recev-pgwRstnotfackpdenied
- tun-recev-discardPgwRstnotfack

The following bulkstats have been added:

- csfb-recev-suspendnotfDiscard
- csfb-recv-suspendnotfNorsp
- csfb-recv-suspendackDiscard
- csfb-recv-resumenotfDiscard
- csfb-recv-resumenotfNorsp
- csfb-recv-resumeackDiscard
- tun-sent-crebear-throttle-succeed
- tun-sent-crebear-throttle-queued
- tun-sent-crebear-throttle-dropped
- tun-sent-retranscrebear-throttle-succeed
- tun-sent-retranscrebear-throttle-queued
- tun-sent-retranscrebear-throttle-dropped
- tun-sent-updbearreq-throttle-succeed
- tun-sent-updbearreq-throttle-queued
- tun-sent-updbearreq-throttle-dropped
- tun-sent-retransupdbearreq-throttle-succeed
- tun-sent-retransupdbearreq-throttle-queued
- tun-sent-retransupdbearreq-throttle-dropped
- tun-sent-delbearreq-throttle-succeed
- tun-sent-delbearreq-throttle-queued
- tun-sent-delbearreq-throttle-dropped
- tun-sent-retransdelbearreq-throttle-succeed
- tun-sent-retransdelbearreq-throttle-queued
- tun-sent-retransdelbearreq-throttle-dropped
- tun-sent-delbearreq-throttle-queued
- tun-sent-delbearreq-throttle-dropped
- tun-sent-retransdelbearreq-throttle-succeed
- tun-sent-retransdelbearreq-throttle-queued
- tun-sent-retransdelbearreq-throttle-dropped
- tun-sent-delbearreq-throttle-dropped
- tun-sent-retransdelbearreq-throttle-hidden
The following bulkstats have been added to reflect incoming throttling:
- msgs-inc-rate-limited
- msgs-inc-rl-scheduled
- msgs-inc-rl-curr-queued
- msg-inc-rl-drop-queue
- msg-inc-rl-throttled
The following GTP path bulkstats have been added for Request Messages:
- total-sent-req
- total-sent-retransReq
- total-recv-req
- total-recv-retransReq
- total-received reqDiscarded
- total-received noRspReq

The following GTP path bulkstats have been added for Response Messages:

- total-sent-rsp
- total-sent-rspAccept
- total-sent-rspDenied
- total-sent-rspRetrans
- total-received resp
- total-received r
- total-received rspAccept
- total-received rspDenied
- total-received rspDiscarded

The following bulkstats have been added:

- mobility-received ctxreqDiscard
- mobility-received ctxreqNorsp
- mobility-received ctxrspDiscard
- mobility-received ctxrspNorsp
- mobility-received ctxackDiscard
- mobility-received idtreqDiscard
- mobility-received idtreqNorsp
- mobility-received idtrspDiscard
- mobility-received fwdrelreqDiscard
- mobility-received fwdrelreqNorsp
- mobility-received fwdrelrspDiscard
- mobility-received fwdacnnottfNorsp
- mobility-received fwdacnnottfDiscard
- mobility-received fwdaccackDiscard
- mobility-received fwdrelcmpnotfDiscard
- mobility-received fwdrelcmpnotfNorsp
- mobility-received fwdrelcompackDiscard
- mobility-received relcancelreqDiscard
- mobility-received relcancelreqNorsp
- mobility-received relcancelsrDiscard
- mobility-received alertmmenottfDiscard
- mobility-received alertmmenottfNorsp
• mobility-recv-alertmmeackDiscard
• mobility-recv-ueactivitynotfDiscard
• mobility-recv-ueactivitynotfNorsp
• mobility-recv-ueactivityackDiscard
• mobility-recv-detachnotfDiscard
• mobility-recv-detachnotfNorsp
• mobility-recv-detachackDiscard
• srvcc-recv-pstocsrspDiscard
• srvcc-recv-pstoscmpnotfDiscard
• srvcc-recv-pstoscancelackDiscard

New in the S-GW Schema

The following bulkstat has been added:
• sessstat-totcur-pdn-paused-charging

Modified S-GW Bulk Statistics

This section identifies S-GW bulk statistics modified in release 15.0.
None for this release.

Deprecated S-GW Bulk Statistics

This section identifies deprecated S-GW bulk statistics that are no longer supported in release 15.0.
None for this release.

New S-GW Output Fields and Counters

This section identifies new S-GW show command output fields and counters available in release 15.0.

show apn-profile full name

Important: This output has been implemented as lab quality.

The following field displays the configuration of the Intelligent Paging for ISR feature, either enabled or disabled.
• ISR-SEQUENTIAL-PAGING

Important: This output has been implemented as lab quality.

The following fields display the configuration of the Overcharge Protection feature.
• Overcharging protection for packet drop count
- Overcharging protection for byte drop count
- Overcharging protection for s1 abnormal release
- Overcharging protection for DDN failure

**show egtpc peers**

The following field has been added to display the Node Features capability of the peer, for the Node functionality GTP Echo feature.
- Node Feature

**show egtp-service all**

The following field has been added to display the node features enabled in each egtpc service, such as PGW Restart Notification, for the Node functionality GTP Echo feature.
- GTPC Node Feature

**show egtpc statistics**

The following two groups of counters have been added to display the number of P-GW Restart Notification Request messages sent and Acknowledgement messages received.
- PGW Restart Notification Request: (total sent, initial sent, and retransmissions sent)
- PGW Restart Notification Ack: (total received, initial received, accepted, denied, and discarded)

**show gtpu statistics peer-address**

The following new fields have been added to this command to display the number of "Supported Extension Header" messages sent and received by the gateway.
- SuppExtnHdr Tx
- SuppExtnHdr Rx

**show lte-policy peer-map name**

The following fields display configuration information of the precedence entries within the specified LTE Policy peer map.
- Peer Map <name>
- precedence <n>

**show peer-profile full all**

The following fields display configuration information for all peer profiles.
- <service-type> Peer Profiles
- Peer Profile Name
- Description
- GTPC echo
• GTPC echo retransmission timeout
• GTPC echo interval
• GTPC max retransmissions
• GTPC retransmission timeout
• Lawful-intercept

**show sgw-service name**

> **Important:** This output has been implemented as lab quality.

The following field has been added to display the configuration of the `ddn isr-sequential-paging delay-time` command:

• `ddn isr-sequential-paging delay-time`

**show sgw-service statistics name**

> **Important:** This output has been implemented as lab quality.

The following field has been added to display the total number of PDNs with charging paused:

• `Paused Charging`

**show subscriber sgw-only full all**

The following field has been added to display the peer profile for this subscriber:

• `Network Peer Profile`

**Modified S-GW Output Fields and Counters**

This section identifies modified S-GW show command output fields and counters available in release 15.0.

None for this release.

**Deprecated S-GW Output Fields and Counters**

This section identifies deprecated S-GW output fields and counters that are no longer supported in release 15.0.

None for this release.
Chapter 22
SNMP MIB Changes in Release 15.0

This chapter identifies SNMP MIB objects and alarms added to, modified for, or deprecated from 15.0 software releases.

SNMP MIB Object Changes as of October 31, 2014

This section provides information on SNMP MIB object changes in release 15.0.

Important: For more information regarding SNMP MIB objects in this section, refer to the SNMP MIB Reference for this release.

New SNMP MIB Objects

This section identifies new SNMP MIB objects available in release 15.0.
None in this release.

Modified SNMP MIB Objects

This section identifies SNMP MIB objects modified in release 15.0.
None in this release.

Deprecated SNMP MIB Objects

This section identifies SNMP MIB objects that are no longer supported in release 15.0.
None in this release.
SNMP MIB Alarm Changes as of October 31, 2014

This section provides information on SNMP MIB alarm changes in release 15.0.

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

### New SNMP MIB Alarms

This section identifies new SNMP MIB alarms available in release 15.0.

The following alarms are new in this release:

- `starThreshMMESessions`
- `starThreshClearMMESessions`
- `starThreshMMEAuthFail`
- `starThreshClearMMEAuthFail`
- `starThreshMMEAttachFail`
- `starThreshClearMMEAttachFail`

### Modified SNMP MIB Alarms

This section identifies SNMP MIB alarms modified in release 15.0.

None in this release.

### Deprecated SNMP MIB Alarms

This section identifies SNMP MIB alarms that are no longer supported in release 15.0.

The following alarms have been deprecated in this release:

- `starThreshTpoRtoTimeout`
- `starThreshClearTpoRtoTimeout`
- `starThreshTpoDnsFailure`
- `starThreshClearTpoDnsFailure`
- `starThreshTpoLowCompressionGain`
- `starThreshClearTpoLowCompressionGain`
SNMP MIB Conformance Changes as of October 31, 2014

This section provides information on SNMP MIB conformance changes in release 15.0.

Important: For more information on regarding SNMP MIB conformances 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 15.0.
None in this release.

Modified SNMP Conformance

This section identifies modified SNMP MIB conformance available in release 15.0.
None in this release.

Deprecated SNMP Conformance

This section identifies modified SNMP MIB units of conformance available in release 15.0.
The following units of conformance have been deprecated in this release:

- starThreshTpoRtoTimeout
- starThreshClearTpoRtoTimeout
- starThreshTpoDnsFailure
- starThreshClearTpoDnsFailure
- starThreshTpoLowCompressionGain
- starThreshClearTpoLowCompressionGain
SNMP MIB Object Changes as of January 31, 2014

This section provides information on SNMP MIB object changes in release 15.0.

**Important:** For more information regarding SNMP MIB objects in this section, refer to the *SNMP MIB Reference* for this release.

### New SNMP MIB Objects

This section identifies new SNMP MIB objects available in release 15.0.

The following objects are new in this release:

- CISCO-ENHANCED-IPSEC-FLOW-MIB
- CISCO-IPSEC-FLOW-MONITOR-MIB

### Modified SNMP MIB Objects

This section identifies SNMP MIB objects modified in release 15.0.

The following objects have been modified in this release:

- starLIRcvryErrType

### Deprecated SNMP MIB Objects

This section identifies SNMP MIB objects that are no longer supported in release 15.0.

None in this release.
SNMP MIB Alarm Changes as of January 31, 2014

This section provides information on SNMP MIB alarm changes in release 15.0.

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

New SNMP MIB Alarms

This section contains new SNMP MIB alarms available in release 15.0.

None in this release.

Modified SNMP MIB Alarms

This section identifies SNMP MIB alarms modified in release 15.0.

None in this release.

Deprecated SNMP MIB Alarms

This section identifies SNMP MIB alarms that are no longer supported in release 15.0.

None in this release.
SNMP MIB Conformance Changes as of January 31, 2014

This section provides information on SNMP MIB conformance changes in release 15.0.

Important: For more information on regarding SNMP MIB conformances 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 15.0.
None in this release.

Modified SNMP Conformance

This section identifies modified SNMP MIB conformance available in release 15.0.
None in this release.

Deprecated SNMP Conformance

This section identifies modified SNMP MIB units of conformance available in release 15.0.
None in this release.
SNMP MIB Object Changes as of November 30, 2013

This section provides information on SNMP MIB object changes in release 15.0.

**Important:** For more information regarding SNMP MIB objects in this section, refer to the *SNMP MIB Reference* for this release.

### New SNMP MIB Objects

This section identifies new SNMP MIB objects available in release 15.0. The following objects are new in this release:

- starMMEInitialDisallowReason

### Modified SNMP MIB Objects

This section identifies SNMP MIB objects modified in release 15.0. The following objects have been modified in this release:

- starChassisType

### Deprecated SNMP MIB Objects

This section identifies SNMP MIB objects that are no longer supported in release 15.0. None in this release.
SNMP MIB Alarm Changes as of November 30, 2013

This section provides information on SNMP MIB alarm changes in release 15.0.

Important: For more information regarding SNMP MIB alarms in this section, refer to the SNMP MIB Reference for this release.

New SNMP MIB Alarms

This section identifies new SNMP MIB alarms available in release 15.0.
None in this release.

Modified SNMP MIB Alarms

This section identifies SNMP MIB alarms modified in release 15.0.
The following alarms have been modified in this release:

- starThreshAAAAacctArchiveQueue-1
- starThreshClearAAAAacctArchiveQueue-1
- starThreshAAAAacctArchiveQueue-2
- starThreshClearAAAAacctArchiveQueue-2
- starThreshAAAAacctArchiveQueue-3
- starThreshClearAAAAacctArchiveQueue-3
- starApsChannelMismatch

Deprecated SNMP MIB Alarms

This section identifies SNMP MIB alarms that are no longer supported in release 15.0.
None in this release.
SNMP MIB Conformance Changes as of November 30, 2013

This section provides information on SNMP MIB conformance changes in release 15.0.

**Important:** For more information regarding SNMP MIB conformances in this section, refer to the *SNMP MIB Reference* for this release.

**New SNMP MIB Conformances**

This section identifies new SNMP MIB units of conformance available in release 15.0.

None in this release.

**Modified SNMP Conformances**

This section identifies modified SNMP MIB units of conformance available in release 15.0.

None for this release.

**Deprecated SNMP Conformances**

This section identifies modified SNMP MIB units of conformance available in release 15.0.

None for this release.
SNMP MIB Object Changes as of September 30, 2013

This section provides information on SNMP MIB object changes in release 15.0.

Important: For more information regarding SNMP MIB objects in this section, refer to the SNMP MIB Reference for this release.

New SNMP MIB Objects

This section identifies new SNMP MIB objects available in release 15.0.

The following objects are new in this release:

- starChassisCrashList
- starPMIPServName
- starPMIPSelfAddrType
- starPMIPSelfAddr
- starPMIPPeerAddrType
- starPMIPPeerAddr
- starPMIPPeerOldRstCnt
- starPMIPPeerNewRstCnt
- starPMIPPeerSessCnt
- starPMIPFailureReason

Modified SNMP MIB Objects

This section identifies SNMP MIB objects modified in release 15.0.

The following objects have been modified in this release:

- starChassisType
- starSlotMappingTable
- starSubMSID
- starSubName
- starSubTimerDuration
- starSubLongDurTimeoutAction
- starSubSetupTime
- starSubHomeAddr
- starSubHomeAddrv6
SNMP MIB Changes as of September 30, 2013

SNMP MIB Object Changes as of September 30, 2013

- starEISServerAddr
- starPortSlot
- starContextName
- starSRPIpAddress
- starThreshNATPortChunks
- starPortSlot

Deprecated SNMP MIB Objects

This section identifies SNMP MIB objects that are no longer supported in release 15.0.

The following objects have been deprecated in this release:

- starSessTtlOctForwarded
- starSessTtlTxBytes
- starSessTtlRxBytes
- starSessTtlSIPTxBytes
- starSessTtlSIPRxBytes
- starSessTtlMIPTxBytes
- starSessTtlMIPRxBytes
- starSessTtlOctForwardedGB
SNMP MIB Alarm Changes as of September 30, 2013

This section provides information on SNMP MIB alarm changes in release 15.0.

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

### New SNMP MIB Alarms

This section identifies new SNMP MIB alarms available in release 15.0.

The following alarms are new in this release:

- starThreshDnsLookupSrvFailure
- starThreshClearDnsLookupSrvFailure
- starThreshHENBGWHenbSessions
- starThreshHENBGWUeSessions
- starThreshClearHENBGWUeSessions
- starThreshHENBGWPagingMessages
- starThreshClearHENBGWPagingMessages
- starApsResponseFail
- starEnhancedCongestionClear
- starChassisCrashListFull
- starECSreaddressServerUp
- starCdrHDDS
- starCdrStreamingStart
- starCdrStreamingComplete
- starVLRDown
- starVLRUp
- starPCFReachable
- starCGWServiceStart
- starECSreaddressServerDown
- starECSreaddressServerUp
- starCdrHDDS
- starCdrStreamingStart
- starCdrStreamingComplete
- starVLRDown
- starVLRUp
- starPCFReachable
- starCGWSVServiceStart
- starCGWSVServiceStop
- starMMENewConnectionsDisallowed
- starMMENewConnectionsAllowed
- starSAMOGServiceStart
- starSAMOGServiceStop
- starCardSwitchoverStart
- starCardSwitchoverComplete
- starCardSwitchoverFailed
- starCardMigrateStart
- starCardMigrateComplete
- starCardMigrateFailed
- starTechSuppPasswdChanged
- starPMIPPathFailure
- starPMIPPathFailureClear

**Modified SNMP MIB Alarms**

This section identifies SNMP MIB alarms modified in release 15.0.
The following alarms have been modified in this release:

- LongDurTimerExpiry
- starEISServerAlive
- starEISServerDead
- starPCFUnreachable
- starLocalUserAdded
- starLocalUserRemoved
- starOsShellAccessed
- starTestModeEntered
- starHiddenAccessEnabled
- starHiddenAccessDisabled
- starPortDown
- starSRPConnDown
- starLAGGroupDown
Deprecated SNMP MIB Alarms

This section identifies SNMP MIB alarms that are no longer supported in release 15.0.

The following alarms have been deprecated in this release:

- starCardSPCSwitchoverStart,
- starCardSPCSwitchoverComplete,
- starCardSPCSwitchoverFailed
- starCardPACMigrateStart,
- starCardPACMigrateComplete,
- starCardPACMigrateFailed
- starCdrHDDStart
- starCdrStreamingStart
- starCdrStreamingComplete
SNMP MIB Conformance Changes as of September 30, 2013

This section provides information on SNMP MIB conformance changes in release 15.0.

**Important:** For more information regarding SNMP MIB conformances in this section, refer to the *SNMP MIB Reference* for this release.

New SNMP MIB Conformances

This section identifies new SNMP MIB units of conformance available in release 15.0. The following conformances have been modified in this release:

- starSessTtlIOctForwardedRev1
- starSessTtlTxBytesRev1
- starSessTtlRxBytesRev1
- starSessTtlSIPTxBytesRev1
- starSessTtlSIPRxBytesRev1
- starSessTtlMIPTxBytesRev1
- starSessTtlMIPRxBytesRev1
- starSessTtlIOctForwardedGBRev1
- starPMIPvPnName
- starPMIPvServName
- starPMIPvSelfAddrType
- starPMIPvSelfAddr
- starPMIPvPeerAddrType
- starPMIPvPeerAddr
- starPMIPvPeerOldRstCnt
- starPMIPvPeerNewRstCnt
- starPMIPvPeerSessCnt
- starPMIPvFailureReason
- starVLRDown
- starVLRUp
- starPCFReachable
- starLIRcvryError
- starLIRcvryComplete
- starCGWServiceStart
- starCGWServiceStop
- starECSreaddressServerDown
- starECSreaddressServerUp
- starThreshHENBGWHenbSessions
- starThreshClearHENBGWHenbSessions
- starThreshHENBGWUeSessions
- starThreshClearHENBGWUeSessions
- starThreshHENBGWPagingMessages
- starThreshClearHENBGWPagingMessages
- starEnhancedCongestionClear
- starChassisCrashListFull
- starMMENewConnectionsDisallowed
- starMMENewConnectionsAllowed
- starSAMOGServiceStart
- starSAMOGServiceStop
- starCardSwitchoverStart
- starCardSwitchoverComplete
- starCardSwitchoverFailed
- starCardMigrateStart
- starCardMigrateComplete
- starCardMigrateFailed
- starPMIPPathFailure
- starPMIPPathFailureClear

Modified SNMP Conformances

This section identifies modified SNMP MIB units of conformance available in release 15.0.

The following conformances have been modified in this release:
- starThreshNATPortChunks
- starThreshClearNATPortChunks
- starCdrStreamingComplete

Deprecated SNMP Conformances

This section identifies modified SNMP MIB units of conformance available in release 15.0.

None for this release.
This chapter identifies system-level features and functionality added to, modified for, or deprecated from 15.0 software releases.

**Important:** All functionality from Limited Availability Release StarOS Version 14.1 has been included in General Availability Release StarOS Version 15.0. The *Cisco ASR 5x00 Release Change Reference, Version 14.1*, details new feature descriptions and configuration, performance, and security changes for the 14.1 release.
System and Platform Enhancements for October 31, 2014

This section identifies all of the system and platform enhancements included in this release:

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

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

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

---

**CSCuo84268 - show egtpc peers needs to be added to the SSD**

*Applicable Products:* All

**Feature Changes**

**Add show egtpc peers Command to List of SDR Strings**

The `show egtpc peers` command has been added to the list of available Support Data Record (SDR) strings that can appear in the list of `show` commands output by the SSD (show support details).

**Performance Indicator Changes**

**show support collection definitions**

The following `show` command strings have been added to the output of this command:

- “show egtpc peers” [Enabled]
- “show egtpc statistics interface cgw-egress” [Enabled]
- “show egtpc statistics interface epdg-egress” [Enabled]
System and Platform Enhancements for February 17, 2014

This section identifies all of the system 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.

---

CSCui80584 - ‘rem_addr’ is not being sent by the ASR to ACS

**Applicable Products:** All

**Feature Changes**

**Sending rem_addr Field in TACACS+ Login Requests**

A Cisco Secure ACS server can be configured to explicitly check the NAS source address for TACACS+ connections. The ASR 5x00 may not properly set the rem_addr field in the TACACS+ protocol packet when initiating a connection with the Cisco Secure ACS server. This may cause the Cisco Secure ACS server to reject the TACACS+ login request.

**Important:** The default behavior is to not fill in the rem_addr field.

A new CLI command enables the setting and sending of the remote address to the IPv4 address associated with the local context management interface for customers who require this field to be verified via the Cisco Secure ACS server.

When enabled the rem_addr field contains the ssh client IP address in ASCII form. If the IP address cannot be retrieved, the length is set to zero.

**Previous Behavior:** Do not send the rem_addr field in TACACS+ protocol.

**New Behavior:** Send the rem_addr field in TACACS+ protocol for use by a Cisco Secure ACS server.

**Customer Impact:** Customers that perform user authentication with NAR filtering must enable this protocol option.

**Command Changes**

`rem_addr client-ip`

This is a new command in the TACACS+ Configuration mode.

`configure`

```
tacacs mode variable
```

```
[ default | no ] rem_Addr client-ip variable
```
end
System and Platform Enhancements for January 31, 2014

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 *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.

CSCui80584 - ‘rem_addr’ is not being sent by the ASR to ACS

Applicable Products: All

**Feature Changes**

Sending rem_addr Field in TACACS+ Login Requests

A Cisco Secure ACS server can be configured to explicitly check the NAS source address for TACACS+ connections. The ASR 5x00 may not properly set the rem_addr field in the TACACS+ protocol packet when initiating a connection with the Cisco Secure ACS server. This may cause the Cisco Secure ACS server to reject the TACACS+ login request.

> **Important:** The default behavior is to not fill in the rem_addr field.

A new CLI command enables the setting and sending of the remote address to the IPv4 address associated with the local context management interface for customers who require this field to be verified via the Cisco Secure ACS server.

When enabled the rem_addr field contains the ssh client IP address in ASCII form. If the IP address cannot be retrieved, the length is set to zero.

**Previous Behavior:** Do not send the rem_addr field in TACACS+ protocol.

**New Behavior:** Send the rem_addr field in TACACS+ protocol for use by a Cisco Secure ACS server.

**Customer Impact:** Customers that perform user authentication with NAR filtering must enable this protocol option.

**Command Changes**

rem_addr client-ip

This is a new command in the TACACS+ Configuration mode.

configure

tacacs mode variable

[ default | no ] rem_Addr client-ip variable
System and Platform Enhancements for November 30, 2013

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 *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.

**CSCue00484 – Syslog - Local event log buffer increase**

Applicable Platforms: ASR 5000, ASR 5500

**Feature Changes**

**Increased Buffer Size for Syslog Events**

The amount of memory for syslog event buffering has been doubled.

**CSCui34979 – icsr adds additional overhead due to SAEGW**

Applicable Products: P-GW, SAE-GW

**Feature Changes**

**ICSR Improvements to Reduce Overhead for SAE-GW**

**Previous Behavior:** There was no microcheckpoint support at P-GW to handle microcheckpoints from S-GW for SAEGW calls. Extra full checkpoints were sent for some scenarios; some full checkpoints with data updated at P-GW only and some with data updated at both S-GW and P-GW.

**New Behavior:** Full checkpoint with partially updated data are no longer being sent. Only those which contain updated data at both S-GW and P-GW are now sent. Microcheckpoint support has been added at P-GW to handle microcheckpoints from S-GW for SAEGW calls.

**CSCui52107 – Reduce idle sec microcheckpoint frequency for improved performance**

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

Reduced Frequency of ICSR UPDATE_IDLESECS Microcheckpoints

**Previous Behavior:** The UPDATE_IDLESECS checkpoint was sent every 30 seconds for inactive users (user idle for more than 60 seconds). UPDATE_IDLESECS is used to calculate the last active tick time (last Activity time) on the standby ICSR chassis. For inactive users, the same last activity time is recalculated whenever this checkpoint is received.

**New Behavior:** UPDATE_IDLESECS is now sent once every 12 minutes for inactive users.

CSCui75767 – SGW full checkpoint to micro checkpoint conversion - Phase 1

**Applicable Products:** S-GW

Feature Changes

S-GW Conversion to ICSR Microcheckpoints Instead of Full Checkpoints

To improve ICSR performance, the S-GW now sends micro checkpoints instead of full checkpoints to the standby chassis for several events.

The following S-GW events are now processed as microcheckpoints:

- UE active to idle transition
- UE idle to active transition (service request for all bearers)
- AMBR Change
- Bearer QoS Change
- Inter eNodeB X2 Handoff
- MME to SGSN Handoff
- MME to SGSN TAU Handoff
- SGSN to MME Handoff
- SGSN to MME TAU Handoff
- Bearer Creation

CSCui91943 - Update default license to include 7 gateways by default

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

Feature Changes

Basic Configuration License Now Supports Additional Gateways

For manufacturing purposes, the basic configuration license supplied with ASR 5x00 hardware platforms now includes default licenses for the following products and features:
- PDSN [ASR5K-00-PN10SW]
- FA [ASR5K-00-FAXXFA]
- RADIUS AAA Server Groups [ASR5K-00-CSXXAAA]
- HA [ASR5K-00-HA10SW]
- MAG [ASR5K-00-GN10HMAG]
- GGSN [ASR5K-00-GN01S]
- ESS [ASR5K-00-GN10SESS]
- DHCP [ASR5K-00-CSXXDHCP]
- IPv4 Routing Protocols [No license required]
- IPSec [ASR5K-00-CS011-K9]
- L2TP LAC [ASR5K-00-PG01L2LA]
- L2TP LNS [ASR5K-00-CS10L2LN]
- Proxy MIP [ASR5K-00-PN01PMIP]
- IPv6 [No license required]
- Lawful Intercept [ASR5K-00-CSXXLI]
- PCF/BS Monitoring [ASR5K-00-CSXXPCFM]
- Dynamic RADIUS extensions (CoA and PoD) [ASR5K-00-CSXXDYNR]
- User Layer3 Tunneling [No license required]
- RADIUS AAA Server Groups [ASR5K-00-CSXXAAA]
- Starent-Only SGSN [No license required]
- PGW [ASR5K-00-PW10GTWY]
- SGW [ASR5K-00-SW10LIC]
- MME [ASR5K-00-ME01BASE]
- Session Recovery [ASR5K-00-PN01REC]
- ASR5500 Initial System SW, Per UDPC [ASR55-00-SWUDPCK9]
- ASR5500 Initial System SW, Per UMIO [ASR55-00-SWUMIOK9]
- SAE GW Bundle [ASR5K-00-SG01 / ASR5K-00-SG10]

Each gateway license – PDSN, HA, SGSN, GGSN, MME, S-GW and P-GW – includes support for up to 500 sessions. You can display the list of licenses by running the `show license info` command.

**Important:** Feature and session licenses purchased and installed by the customer will override these default base-level keys.
System and Platform Enhancements for October 30, 2013

System Feature Changes as of October 30, 2013

This section provides information on system feature changes in release 15.0.

Important: For more information regarding features in this section, refer to the System Administration Guide for this release.

New System Features

This section identifies new system features available in release 15.0.

None for this release

Modified System Features

This section identifies system features modified in release 15.0.

ICSR Improvements to Reduce Overhead for SAE-GW

Previous Behavior: There was no microcheckpoint support at P-GW to handle microcheckpoints from S-GW for SAEGW calls. Extra full checkpoints were sent for some scenarios; some full checkpoints with data updated at P-GW only and some with data updated at both S-GW and P-GW.

New Behavior: Full checkpoint with partial updated data are no longer being sent. Only those which contain updated data at both S-GW and P-GW are now sent. Microcheckpoint support has been added at P-GW to handle microcheckpoints from S-GW for SAE-GW calls.

Increased Buffer Size for Syslog Events

The amount of memory for syslog event buffering has been doubled.

Reduced Frequency of ICSR UPDATE_IDLESECS Microcheckpoints

Previous Behavior: The UPDATE_IDLESECS checkpoint was sent every 30 seconds for inactive users (user idle for more than 60 seconds). UPDATE_IDLESECS is used to calculate the last active tick time (last Activity time) on the standby ICSR chassis. For inactive users, the same last activity time is recalculated whenever this checkpoint is received.

New Behavior: UPDATE_IDLESECS is now sent once every 12 minutes for inactive users.

System Command Changes as of October 30, 2013

This section provides information on system-level command changes in release 15.0.

None for this release.
System Performance Indicator Changes as of October 30, 2013

This section provides information on system-level performance indicator changes in release 15.0. None for this release.

System Security Management Changes as of October 30, 2013

This section provides information on system-level security management changes in release 15.0. None for this release.
System and Platform Enhancements for September 30, 2013

System Feature Changes as of September 30, 2013

This section provides information on system feature changes in release 15.0.

**Important:** For more information regarding features in this section, refer to the *System Administration Guide* for this release.

New System Features

This section identifies new system features available in release 15.0.

**BGP MPLS VPNv6**

The ASR 5x00 supports VPNv6 as described in RFC 4659 – *BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN*.

An IPv6 VPN is connected over an IPv6 interface or sub-interface to the Service Provider (SP) backbone via a PE router. The site can be both IPv4 and IPv6 capable. Each VPNv6 has its own address space which means a given address denotes different systems in different VPNs. This is achieved via a VPNv6 address-family which prepends a Route Distinguisher (RD) to the IP address.

A VPNv6 address is a 24-byte quantity beginning with an 8-byte RD and ending with a 16-byte IPv6 address. When a site is IPv4 and IPv6 capable, the same RD can be used for the advertisement of both IPv4 and IPv6 addresses.

The system appends RD to IPv6 routes and exchanges the labeled IPv6-RD using the VPNv6 address-family. The Address Family Identifier (AFI) and Subsequent Address Family Identifier (SAFI) fields for VPNv6 routes will be set to 2 and 128 respectively.

The IPv6 VPN traffic will be transported to the BGP speaker via IPv4 tunneling. The BGP speaker advertises to its peer a Next Hop Network Address field containing a VPN-IPv6 address whose 8-octet RD is set to zero and whose 16-octet IPv6 address is encoded as an IPv4-mapped IPv6 address (RFC 4291) containing the IPv4 address of the advertising router. It is assumed that only EBGP peering will be used to exchange VPNv6 routes.

For additional information see the descriptions for the following CLI commands:

- address-family
- ipv6 pool
- show ip bgp neighbors
- show ip bgp vpnv6
- show mpls ftn

For additional information refer to the *System Administration Guide*.

CLI Autoconfirmation
By default, the system is configured to prompt all administrative users with a confirmation prior to executing certain commands. This functionality serves two purposes:

- Helps ensure that you do not execute an unwanted configuration change.
- Indicates potential misspellings of names during configuration. The first time you configure an element name (context, subscribers, services, etc.), the prompt is displayed. The prompt is not displayed for subsequent entries of the name. Therefore, if you see the confirmation prompt after entering the name of a previously configured element, it is likely that you misspelled the name.

You can control CLI autoconfirmation at the following levels:

- **Specific administrative user sessions**: To enable or disable autoconfirmation, use the `[no] autoconfirm` commands while in the Exec Mode.
- **All Future Sessions**: To disable or re-enable autoconfirmation for all future sessions, use the `[no] autoconfirm` commands while in the Global Configuration Mode.
- **For specific commands**: Disable autoconfirmation for various commands that support the `-noconfirm` keyword, such as the save configuration or card reboot commands.

### Configurable Subscriber State Management Audit Process (ICSR)

A new `audit` command and keywords in Context Configuration mode allow an operator to specify the start time and periodicity for generating Interchassis Session Recovery (ICSR) Service Redundancy Protocol (SRP) audit statistics. This audit ensures that two ICSR peers are in synch and identifies any discrepancies prior to scheduled or unscheduled switchover events.

### Demux Functionality on MIO/UMIO (ASR 5500)

This feature allows an MIO/UMIO card to host all the demux tasks on StarOS. Previously one DPC in the system could be reserved as a demux card where none of the session components directly related to subscribers are running. This feature frees session subsystem resources to increase system performance and throughput.

This feature is disabled by default and can be enabled via the Global Configuration mode `require demux card` command which has been modified for this purpose.

The following restrictions apply when enabling an MIO/UMIO as a demux card:

- The `require demux management-card` command must be configured before any service or contexts have been created on the system. The command will not execute after a mode of operation has been selected for the chassis.
- Only the following services currently support the designation of an MIO/UMIO card for demux functions: GGSN, SGW, PGW, HA and SAE-GW.
- Ex-GW, L2TP, MME, NEMO and SGSN are not supported.
- After the ASR 5500 has booted with demux functions running on an MIO/UMIO, you cannot configure non-supported services. A maximum of eight Demux Managers are supported. Any attempt to add more than eight Demux Managers will be blocked.
- Service/products requiring a large number of VPN Managers, VRFs and/or Demux Managers must not enable demux functions on an MIO.
- With demux functions running on an MIO, the ASR 5500 supports a maximum of 10 contexts, 15 interfaces per context, with a maximum of 64 interfaces and 250 VRFs per system.

To support this feature session recovery must also be enabled via the Global Configuration mode `require session recovery` command.
**Important:** After enabling demux card and session recovery, you must save the configuration and reboot the ASR 5500 to enable this feature.

Implementation of this feature assumes that CEPS (Call Events Per Second) and the number of subscribers will remain constant, but the data rate will increase. This ensures that the CPU demand will not increase on the MIO.

**Caution:** Enabling the Demux on MIO/UMIO feature changes resource allocations within the system. This directly impacts an upgrade or downgrade between StarOS versions in ICSR configurations. Contact Cisco TAC for procedural assistance prior to upgrading or downgrading your ICSR deployment.

**Important:** Contact Cisco TAC for additional assistance when assessing the impact to system configurations when enabling the Demux on MIO/UMIO feature.

### Enabling Password Access to cli-test commands

A Security Administrator can set a plain-text or encrypted password for access to CLI test commands. The password value is stored in `/flash` along with the boot configuration information. The `show configuration` and `save configuration` commands will *never* output this value.

The Global Configuration mode command `tech-support test-commands [encrypted] password <password>` sets an encrypted or plain-text password for access to CLI test-commands.

When a test-commands password is enabled, the Global Configuration mode command `cli test-commands [encrypted] password <password>` requires the entry of the password keyword. If the `encrypted` keyword is specified, the `<password>` argument is interpreted as an encrypted string containing the password value. If the `encrypted` keyword is not specified, the `<password>` argument is interpreted as the actual plain text value.

**Important:** If `tech-support test-commands password` is never configured, `cli-test commands` will always fail. If the `password` keyword is not entered for `cli-test-commands`, the user is prompted (no-echo) to enter the password. Also, `cli hidden` must be enabled by a Security Administrator to access the CLI test-commands.

### New Chassis ID Encryption Method

Beginning with this release, the chassis ID will be generated from an input chassis key using the SHA2-256 algorithm followed by base36 encoding. The resulting 44-character chassis ID will be stored in the same chassisid file in flash.

Release 14 and Release 15 chassis IDs will be in different encryption formats. Release 15 will recognize a Release 14 chassis ID and consider it as valid. Upgrading from 14.x to 15.0 will not require changing the chassis ID or configuration file.

However, if the chassis key is reset in Release 15 through the setup wizard or `chassis-key` CLI command, a new chassis ID will be generated in Release 15 format (44 instead of 16 characters). Release14 builds will not recognize the 44-character chassis ID. If the chassis is subsequently downgraded to Release 14, a new 16-character chassis ID will be generated. To accommodate the old key format, you must save the configuration file in pre-v12.2 format before the downgrade. If you attempt to load a v15 configuration file on the downgraded chassis, StarOS will not be able to decrypt the password/secrets stored in the configuration file.

For additional information, refer to the *System Administration Guide*.

### Selectable Password/Secrets Encryption Algorithm
An administrator can now specify the type of encryption algorithm to be used for passwords and secrets. The default algorithm will be the MD5-based cipher (algorithm “A”) used in release 14.0. Another option specifies the use of AES-CBC-128 for encryption and HMAC-SHA1 for authentication (algorithm “B”).

Use the Global Configuration mode `cli-encrypt-algorithm` command to specify the desired encryption algorithm – A (default) or B. For additional information, refer to the Command Line Interface Reference.

**Support Data Collector**

The Support Data Collector (SDC) is a system feature that allows scheduled collection of process state, counter, event and attribute data that may be useful when troubleshooting problems at an installation site.

The task of collecting the support data is performed by a background CLI task called the record collector. The administrator configures the SDC via the CLI with the commands to be executed on a periodic basis. The record collector always runs in the background and checks if there are records to be collected.

When it is time to collect support data, the scheduler executes the configured sequence of CLI commands and stores the results in a gunzipped (.gz) file on the hard-disk. This file is called an SDR (Support Data Record), and represents a snapshot of the overall state of the system at that time.

The Support Data Collector (SDC) is a system feature that allows scheduled collection of process state, counter, event and attribute data that may be useful when troubleshooting problems at an installation site.

Technical Assistance Center (TAC) personnel and local administrators can review the SDRs on-line or by transferring them off the system. They may also wish to investigate the collector state information. The figure below shows system tasks that contain state and counter information. Arrows between tasks and processes represent messenger requests and indicate the predominant flow of data.

For additional information see the descriptions for the following CLI commands:

- `support collection`
- `support record`
- `show support collection`
- `show support record`
- `delete support record`

For additional information refer to the System Administration Guide.

**Support for Universal MIOs and DPCs (ASR 5500)**

Universal card types (UMIO and UDPC) are now supported on the ASR 5500 platform. A special license that contains the correct number of universal cards must be purchased and installed on the system. With this license UMIOs and UDPCs can also be added to an ASR 5500 chassis that was previously equipped with MIOs and DPCs. Refer to the latest version of the *ASR 5500 Installation Guide* for descriptions of UMIO cards and UDPCs. For information on licensing requirements, contact your Cisco account representative.

**IPSec Common Features**

*Important:* The commands associated with this feature appear in the CLI for this release. However, they have not been qualified for use with any current Cisco StarOS gateway products.

A number of IPSec features an enhancements have been added in support of Wireless Security Gateway development. These features appear in this StarOS release and are included in the StarOS Standalone Instance (SSI) build.

The following is a list of these features with brief descriptions:
• **Multiple Child SA (MCSA) Support** – The creation of multiple child SAs helps an operator to segregate and limit the secure traffic into multiple flows. For example, control and data paths between two nodes can be established over two child SAs; the rest of the data between the nodes will bypass IPSec. Multiple child SAs may be used for carrying traffic with different class of services (QoS). Similarly, different SAs could be used to carry different traffic with specific security properties.

• **Certificate Management Protocol (CMPv2)** – The Certificate Management Protocol (CMP) is an Internet protocol used for obtaining X.509 digital certificates in a public key infrastructure (PKI). It is described in RFC 4210. StarOS implements the subset of CMPv2 functions:
  
  - **Key pair and X.509 certificate request generation**: The StarOS security gateway acts as an end entity as described in RFC 4210. The gateway generates the X.509 public and private key pair for authentication during IKE AUTH. It generates the public and private keys using OpenSSL libraries. The generated private key is saved locally on the management card, and the public key is embedded in the generated X.509 certificate request. The key uses RSA encryption; SHA-1 with RSA encryption is used on the Hashing function for the generated certificate. Certificate requests are sent to the Certificate Authority (CA) or Registration Authority (RA) during the certification process via CMPv2.
  
  - **Initial certificate request transaction (ir and ip)**: A certificate request triggers the CMPv2 messaging to get the first certificate certified by the Certification Authority (CA). This CMPv2 transaction is identified by the Certification Request and Certification Response messages (ir and ip). At the end of this transaction the security gateway may receive the certificate signed by the CA in the response message. This certificate is then saved in the management card and is also propagated to the packet processing cards via internal messaging. The IKEv2 tunnel creation done at the packet processing cards requires this certificate for the IKE_AUTH transaction.
  
  - **Certificate enrolment (cr and cp)**: This CMPv2 transaction obtains additional certificates certified by CA after the initial certification is done. The security gateway triggers additional certificate enrolment. The additional certificates are saved and used in a manner similar to the initial certificate.
  
  - **Polling request and response (pollReq and pollRep)**: The ir, cp or the kup message received from the CA may contain a status code of “waiting”. This indicates that the CA is still evaluating the certificate request and will require more time to sign the certificate. In this case the security gateway sends a pollReq message to the CA. The pollRep message from the CA may either contain the signed certificate or indicate a status of “waiting” again. If the pollRep message contains the certificate, it is treated as an ir/cp/kup message with a signed certificate and all relevant actions are taken. The security gateway also supports a CLI command to manually trigger polling for any request.
  
  - **Certificate update transaction (kur and kup)**: This key pair update transaction re-certifies or updates a public/private key pair of the certificate after or before its validity expires. The Key Update Request (kur) message is sent to the CA with a certificate having a new public key, and the CA sends a Key Pair Update Response (kup) message with the signed certificate. The security gateway also supports two mechanisms to update an existing certificate:
    
    - **Manual Update**: The gateway sports a CLI command to trigger the certificate update transaction.
    
    - **Auto update**: The gateway can be configured to automatically trigger a certificate update a specified number of days before the certificate expires.

    For both manual and automatic updates, the updated certificate is saved on the management card and propagated to the packet processing cards.

- **Online Certificate Status Protocol (OCSP)** – OCSP provides a facility to obtain timely information on the status of a certificate (RFC 2560). OCSP messages are exchanged between a gateway and an OCSP responder during a certificate transaction. The responder immediately provides the current status of the presented certificate. The status can be good, revoked or unknown. The gateway can then proceed based on the response.
- **Access Control via Blacklist or Whitelist** – A blacklist or block list is a basic access control mechanism that allows everyone access, except for the members of the black list. The opposite is a whitelist, which denies access to everybody except for members of the white list. You can implement either a blacklist or whitelist; both listing techniques cannot be implemented simultaneously on a security gateway.

- **PSK Support for Remote Secrets** – StarOS also allows the operator to configure a remote secret list that contains PSKs based on remote ID types. The remote secret list can contain up to 1000 entries; only one remote secret list is supported per system. The remote secret list bound to a crypto map and/or crypto template.

- **CA Certificate Chaining** – Certificate chaining, also known as hierarchical CA cross certification, is a method by which an entity is authorized by walking a sequence of intermediate As up to the trust-point CA. An intermediate CA is a certification authority under a root CA, which is a self-signed authority. StarOS only supports X.509 Certificate encoding when sending certificates with a maximum certificate chain length of 4. The length of the certificate chain is defined as the number of all certificates in the chain, including the entity and intermediate CA certificates, but excluding the trust anchor certificate.

- **IKEv2 RFC 5996 Compliance** – Staros IKEv2 has been enhanced to comply with RFC 5996 – Internet Key Exchange Protocol Version 2 (IKEv2). RFC 5996 introduces two new notification payloads using which certain conditions of the sender can be notified to the receiver. The IANA assigned numbers for these payloads are as follows:
  - TEMPORARY_FAILURE – IANA Assigned Number = 43
  - CHILD_SA_NOT_FOUND – IANA Assigned Number = 44

- **Rekey Traffic Overlap** – To assure interrupt-free traffic IKE SA and IPSec SAs have to be “rekeyed”. By definition, rekeying is the creation of new SA to take the place of expiring SA well before the SA expires. RFC 5996 describes the procedure for IKEv2 rekeying with minimal traffic loss. During the rekeying, both initiator and responder maintain both SAs for some duration during which they can receive (inbound) on both SAs. The inbound traffic on the old SA stops only after each node unambiguously knows that the peer is ready to start sending on the new SA (switch outbound to new SA).

- **CRL Fetching** – Certificate Revocation Lists are issued periodically by the CA. This list contains the serial number of all the certificates that are revoked. An operator can verify the status of a certificate using a CRL. A CRL can be fetched via LDAPv3 from a CRL issuer (Trusted by CA). When configured, this function also re-fetches the CRL once it expires in the cache. If the CRL is obtained from a CRL Distribution Point (CDP), StarOS defers the CRL fetch until the tunnel is established.

- **Reverse DNS Lookup for Peer IP** – A CLI command enables a DNS reverse look up from the IKE peer IP address to the hostname. A DNS query is sent to obtain the IKE Peer name from DNS Server. The IP address-to-host name mapping appears when displaying the statistics.

For additional information refer to [System Security Management Changes as of September 30 2013](#), the [System Administration Guide](#) and [StarOS IP Security Reference](#).

### Modified System Features

This section identifies system features modified in release 15.0.

### SRP Peer Groups

BGP is employed with Interchassis Session Recovery (ICSR) configurations linked via Service Redundancy Protocol (SRP). By default an ICSR failover is triggered when all BGP peers within a context are down.

Optionally, you can configure SRP peer groups within a context. ICSR failover would then occur if all peers within a group fail. This option is useful in deployments in which a combination of IPv4 and IPv6 peers are spread across multiple paired VLANs, and IPv4 or IPv6 connectivity is lost by all members of a peer group.
For additional information see the descriptions for the following CLI commands:

- monitor authentication-probe
- monitor bgp
- monitor diameter
- show srp monitor

Also see the System Administration Guide and Command Line Reference.

### VRFs and IPv6 Pools per Context

**Previous Behavior**: Prior to this release, you could only configure 250 VRFs and 32 IPv6 pools per context.

**New Behavior**: With this release you can configure up to 300 VRFs and 256 IPv6 pools context.

### System Command Changes as of September 30, 2013

This section provides information on system-level command changes in release 15.0.

**Important**: For more information regarding commands in this section, refer to the Command Line Interface Reference for this release.

### New System Commands

This section identifies new system commands available in release 15.0.

**audit**

Use this command and its keywords to specify the start time and periodicity for generating ICSR SRP audit statistics.

```
config

    context ctx_name

    service-redundancy-protocol

    audit daily-start-time 06 00

    audit periodicity 90

end
```

**busyout ipv6 pool**

Use this command and its keywords to busyout IPv6 pools.

```
config

    context ctx_name
```
System Changes in Release 15.0

System and Platform Enhancements for September 30, 2013

busyout ipv6 pool { all | all-dynamic | all-static | name pool_name } [ address-range start_address end_address | lower-percentage percent | upper-percentage percent ]

cli-encrypt-algorithm

Specify MD5-based cipher ("A") or AES-CBC-128 for encryption and HMAC-SHA1 for authentication ("B") when encrypting passwords and secrets.

config

   cli-encrypt-algorithm { A | B }

   default cli-encrypt-algorithm

end

ip vrf-list

Use this command to create a VRF list and add VRFs to the list. The VRFs must have been previously created via the ip vrf command. This command supports multiple VRFs over NEMO.

configure

   context ctx_name

   ip vrf-list list_name permit vrf_name

end

mpls exp

The mpls exp command sets the default behavior as Best Effort using a zero value in the 3-bit MPLS EXP (Experimental) header. This value applies to all the VRFs in the context. The default behavior is to copy the DSCP value of mobile subscriber traffic to the EXP header, if there is no explicit configuration for DSCP to EXP (via the mpls map-dscp-to-exp dscp <n> exp <m> command).

This command disables the default behavior and sets the EXP value to the configured <value>.

configure

   context ctx_name

   mpls exp <value>

end

support collection

The support collection command modifies and/or enables the support collection process. If support collection has been previously disabled, this command enables the collection activity. If the support collection is currently enabled, this command may be used to modify the sleep-duration interval and/or the maximum number of SDRs that can be collected and stored.

configure
support collection [ sleep-duration [ hours <h> | minutes <m> ] ] [ max-records <n> ]

no support collection

default support collection

end

Notes:

- The **support collection** command modifies and/or enables the support collection process. If support collection has been previously disabled, this command enables the collection activity. If the support collection is currently enabled, this command may be used to modify the sleep-duration interval and/or the maximum number of SDRs that can be collected and stored.

- The **sleep duration** keyword specifies the time interval between the collection of support data. It can be specified in hours or minutes with a default of one hour (60 minutes).

- The **max-records** keyword specifies the number of SDRs to store as an integer from 1 to 65535. When this value is exceeded, the new SDR overwrites the oldest SDR. The default value is 168.

**support record**

The **support record section** command configures a specific record section or set of record sections for a support information output command. The order in which the record section commands are specified defines the order in which the collected support data record sections are saved.

configure

```
support record section <section-name> command "<command-string>" [ section <section-name> command "<command-string>" ] ...
```

no support record [ all | section <section_name> ]

default support record [ all | section <section_name> ]

Note:

- If the **support record section** command is not explicitly configured by the user, a default set of record section commands are used. These default record section commands are displayed when you run the **show configuration verbose** command. If support record section commands are explicitly configured, they replace the default commands.

**tech-support test-commands password**

Sets the password required to execute the **cli test-commands** command in the Exec and Global Configuration mode.

```
config

tech-support test-commands [encrypted] password password

no tech-support test-commands password
```

end
**Important:** An SNMP trap is generated when an administrator enters or edits a password via this command (starTechSupportPasswordChanged).

**Important:** Access to the cli test-commands command also requires that a Security Administrator or Administrator enabled the Global Configuration mode cli hidden command.

**Modified System Commands**

This section identifies system commands modified in release 15.0.

**clear task resources max**

A new max keyword has been added to the clear task resources command. It clears just the maximum usage levels for tasks as opposed to all current usage levels.

```plaintext
clear task resources { card card_num { facility facility { all | instance id max } | facility facility { all | instance id max } | max }
```

**delta-route-modifier**

Specifies the delta that will be used to compute the route modifier difference between the active and standby chassis. Prior to this release, the delta is applied only in the standby state. For this release, it is used in both states.

```plaintext
configure

    configure context ctx_name

    service-redundancy-protocol

    delta-route-modifier value

end
```

**ipv6 prefix pool**

A prefix-length option has been added to this command to set configured prefix lengths of 48, 52, 56 or 64 bits. The default is 64 bits. This option supports S-GW/P-GW validation of fixed-length addresses via DHCPv6 (TS 29.274 – 7.2.2 and 8.14).

```plaintext
configure

    configure context ctx_name

    ipv6 pool name range ipv6_address prefix-length prfx_length

end
```

**monitor authentication-probe**
An optional `group` keyword has been added to this command in support of SRP peer grouping for ICSR configurations.

```bash
configure
  configure context ctx_name
  service-redundancy-protocol
    monitor authentication-probe context context_name { ipv4_address | ipv6_address } [ group group_id ] [ port port_number ]
  end

monitor bgp
An optional `group` keyword has been added to this command in support of SRP peer grouping for ICSR configurations.

```bash
configure
  configure context ctx_name
  service-redundancy-protocol
    monitor bgp context context_name { ipv4_address | ipv6_address } [ group group_id ] [ vrf vrf_name ]
  end
```

monitor diameter
An optional `group` keyword has been added to this command in support of SRP peer grouping for ICSR configurations.

```bash
configure
  configure context ctx_name
  service-redundancy-protocol
    monitor diameter context context_name endpoint endpoint_name [ fqdn fqdn | group group_id ] peer { ipv4_address | ipv6_address } [ port port_number ]
  end
```

monitor subscriber
The INBOUND and OUTBOUND portions of the output of the Exec mode `monitor subscriber` command are now prefaced with the date in DoW MMMM DD YYYY format.

```bash
monitor subscriber [ asa-peer-address bs_peer_address | callid call_id fng-peer-address ipv4_address imei imei_value | imsi imsi_value ipaddr ip_address | ipv6addr ipv6_address | ipsg-peer-address ipsg_peer_address| msid ms_id | msisdn msisdn | next-call pcf pcf_address | pdif-peer-address pdif_peer_address peer-fa peer_fa_address | peer-lac lac_peer_address | sgsn-address sgsn_address | type { lxrtt asangw asnpc | closedrp evdorev0 evdoreva | interrogating-cscf ggsn [ Next-Call By APN ] | ha |
**require demux card management-card**

This command transitions the standby MIO/UMIO card in an ASR 5500 to host all the demux tasks on StarOS. It is enabled via the `require demux card management-card` command.

```plaintext
configure

   require demux card [ management-card | processing-card ]

   end
```

Note:

- Demux card functionality is disabled by default on the ASR 5500 and ASR 5000. The `require demux card management-card` command is only supported for GGSN, P-GW, S-GW, HA and SAEGW running on an ASR 5500; it is not supported on the ASR 5000 for any product. This feature is explicitly not supported for Ex-GW, MME and SGSN because these products use a higher proportion of MIO/UMIO CPU resources.

- To support this feature session recovery must also be enabled via the Global Configuration mode `require session recovery` command on the ASR 5500.

- Running `require demux card processing-card` dedicates a DPC/UDPC to run demux functions in the ASR 5500.

**Important:** After enabling demux card and session recovery, you must save the configuration and reboot the ASR 5500 to enable demux card functions on the standby MIO/UMIO card.

**shutdown**

The `shutdown` command for Ethernet ports has been modified to power down ports on FELC, GELC and QGLC line cards (ASR 5000). This command already powers down ports on MIO/UMIO cards (ASR 5500).

```plaintext
configure

   port ethernet slot_number/port_number

      shutdown

   end
```

**Deprecated System Commands**

This section identifies system commands that are no longer supported in release 15.0.

**hidden password**

This debug level command has been deprecated in this release. Its functionality has been replaced by the newly added `tech-support test-commands` command.
System Performance Indicator Changes as of September 30, 2013

This section provides information on system-level performance indicator changes in release 15.0.

**Important:** For more information regarding bulk statistics and output fields and counters in this section, refer to the *Statistics and Counters Reference* for this release.

### New System Bulk Statistics

This section identifies new system bulk statistics available in release 15.0.

### New in the ICSR Schema

The following new statistics support ICSR functionality:

- switchover-number
- switchover-time
- switchover-reason
- switchover-duration
- total-num-act-calls-swo-time
- total-num-lost-calls-swo-time
- checkpoints-never-sent
- checkpoints-send-failed
- audit_number
- audit_chassis_state
- audit_start_time
- audit_duration
- audit_reason
- total_audit_active_sessions
- total_audit_new_sessions
- total_audit_stale_sessions
- total_audit_inactive_sessions
- total_sessmgr
- total_sessmgr_active_connected
- total_sessmgr_standby_connected
- total_sessmgr_pending_connected
- total_sess_crr_count
- total_sess_crr_pre_installed
New in the System Schema

A new disconnect reason, disc-reason-552, has been added to this schema:

- sgsn-dbr-cause-isr-deact-detach(552)

Modified System Bulk Statistics

This section identifies system bulk statistics modified in release 15.0.

None for this release.

Deprecated System Bulk Statistics

This section identifies system bulk statistics that are no longer supported in release 15.0

Deprecated in the System Schema

The following bulk statistics are deprecated for this release:

- asngw-cur-active-call
- asngw-total-sess-setup
- asngw-retriesexhaust
- asngw-sfs
- asngw-tidfail
- asngw-handoffattempt
- asngw-handoffdenied
- asngw-handoffcomp
- asngw-authsucc
- asngw-authfailures
- asngw-simple-ip-reanchored
- asnpc-cursess
- asnpc-curactive
- asnpc-ttlsetup
- asnpc-retriesexhaust
- asnpc-tidfail
- asnpc-luattempted
- asnpc-ludenied
- asnpc-lucomp
- asnpc-pagattempted
- asnpc-pagsucceeded
- asnpc-annoucetriggered
• asnpc-imexitresponsetopaging
• asnpc-noresponsetopaging
• phsgw-cursess
• phsgw-cur-active-call
• phsgw-total-sess-setup
• phsgw-retriesexhaust
• phsgw-uplink-sfs
• phsgw-downlink-sfs
• phsgw-tidfail
• phsgw-handoffattempt
• phsgw-handoffdenied
• phsgw-handoffcomp
• phsgw-authsucc
• phsgw-authfailures
• phsgw-3partyauthsucc
• phsgw-3partyauthfailures
• phspc-cursess
• phspc-total-sess-setup
• phspc-retriesexhaust
• phspc-tidfail
• phspc-locupdate-attempt
• phspc-locupdate-denied
• phspc-locupdate-comp
• phspc-paging-attempt

New System Output Fields and Counters

This section identifies new system output fields and counters available in release 15.0.

show ip vrf-list

This command displays information about all VRF lists or a specified VRF list.

• List name(s)
• VRF names

show support collection

The show support collection command displays information on SDC activity. It display informations such as the start time of the last scheduled collection, the duration of the last scheduled collection, whether the collection is still in
progress, etc. In addition this command lists the currently stored set of SDR record-ids, their respective timestamps, and size of each SDR.

```
show support collection [ definitions ]
```

The optional definitions keyword displays the list of default support record section definitions. This is the list of all valid record section definitions. The display also indicates whether the record section is enabled or disabled by default.

**show support record**

The `show support record` command displays a collection of SDRs. The SDRs are displayed in order from lowest record-id to highest record-id.

Each SDR is identified by a time index called the record-id. For example, the most recent record is always record-id 0 (filename = sdr.0.gz). The next older record is record-id 1 (filename = sdr.1.gz), and so on.

When a new record is collected it is given a record-id of 0. The previously most recent record is renamed to record-id 1, and so on. The display includes the record-id along with the collection time-stamp.

```
show support record <record-id> [ to <record-id> ] [ section <section_name> ]
```

**delete support record**

The `delete support record` command removes an SDR with specified record-id or all SDRs in the specified range of record-ids.

```
delete support record <record-id> [ to <record-id> ]
```

**Modified System Output Fields and Counters**

This section identifies system output fields and counters modified in release 15.0

**show ipv6 pool [verbose]**

The output of this command has been modified to display the following additional information:

- Busyout: (B) - Busyout Configured
- Busy-Out Range Configured [verbose]
- Total Busy-Out usage [verbose]

**show mpls ilm**

The following keywords have been added to this command:

- `fec` – displays the MPLS Incoming Label Map (ILM) table with Forward Equivalency Class (FEC) information.
- `label label_value` – displays the MPLS IHM table with information for the specified label.
- `verbose` – displays detailed information from the MPLS ILM table.

**show session disconnect-reasons**

The output of this command has been modified to display the following additional information:
System Changes in Release 15.0

System and Platform Enhancements for September 3, 2013

- sgn-dbr-cause_isr-deact-detach(552)

show srp monitor

The output of this command has been modified to display the GroupID for the SRP peer group associated with an IP address in the Context.

show srp monitor

show support details (SSD)

The output of this command has been modified to also display the output of show session counters historical all by default.

show support details

show version

The output of this command now includes the “Image Branch Version” in CDETS format [NNN.NNN (NNN)].

Deprecated System Output Fields and Counters

This section identifies system output fields and counters that are no longer supported in release 15.0.

None for this release.

System Security Management Changes as of September 30, 2013

This section provides information on system-level security management changes in release 15.0.

Important: For more information regarding commands in this section, refer to the Command Line Interface Reference and StarOS IP Security Reference for this release.

Important: The commands described in this section appear in the CLI for this release. However, they have not been qualified for use with any current Cisco StarOS gateway products.

New System Security Commands

This section identifies new system security commands available in release 15.0. The commands listed below are associated with IPSec Common features added in support of Security Gateway (SeGW) operations.

Exec Mode

The following Exec Mode commands have been added in support of IPSec Common Features.

cmp initialize modulus
Triggers a Key Update Request after generating a public and private key pair, as well an X.509 certificate to be included in the Key Update Request for a certificate that is about to expire. This is a Certificate Management Protocol v2 command.

```
cmp initialize modulus mod_type cert-name name subject-name "subject_string" ca-psk key ca-root ca_name ca-url url
```

cmp enroll current-cert

Triggers a Certification Request (CR) after generating a public and private key pair, as well as an X.509 certificate to be included in the CR for a second certificate from the same Certificate Authority (CA).

```
cmp enroll current-cert old-cert-name modulus mod_type subject-name "subject_string" cert-name name ca-root ca_name ca-url url
```

cmp update current-cert

Triggers a Key Update Request after generating a public and private key pair, as well an X.509 certificate to be included in the Key Update Request for a certificate that is about to expire. This is a Certificate Management Protocol v2 command.

```
cmp update current-cert old-cert-name modulus mod_type ca-root ca_name ca-url url
```

cmp fetch current-cert

This command is only applicable for the ASR 9000 platform. CMPv2 operations are performed only on one Virtual Services Module (VSM) in the chassis. The certificates along with the private key file and the root certificate are stored on the supervisor card. When invoked on other VSMs in the chassis, this command reads the certificate, private key and the root certificate from the supervisor card.

```
cmp fetch current-cert old-cert-name ca-root ca_name
```

cmp poll current-cert

Triggers a pollReq for the specified certificate.

```
cmp poll current-cert old-cert-name
```

crypto blacklist file update

Updates the blacklist (access denied) file using the path specified when the blacklist was enabled.

```
crypto blacklist file update
```

crypto whitelist file update

Updates the whitelist (access granted) file using the path specified when the whitelist was enabled.

```
crypto whitelist file update
```

Global Configuration Mode

The following Global Configuration Mode commands have been added in support of IPSec Common Features.
**cmp auto-fetch**

Use this command to add a fetch configuration for each certificate for which automatic update is required. This is a Certificate Management Protocol v2 command.

```plaintext
configure

cmp auto-fetch current-name cert_name ca-root ca_name time days
```

**cmp cert-store**

Use this command to add a file location on /flash disk where the certificates and private keys will be stored. This is a Certificate Management Protocol v2 command.

```plaintext
configure

cmp cert-store location pathname [key reuse]
```

**cmp cert-trap time**

Defines when an SNMP MIB certificate expiry trap should be sent as the number of hours before expiration.

```plaintext
configure

cmp cert-trap time hours
```

**crypto blacklist file**

Configures a blacklist (access denied) file to be used by a security gateway (SeGW).

```plaintext
configure

crypto blacklist file pathname
```

**crypto remote-secret-list**

Specifies the name of the remote secret list for storing remote secrets based on the ID type. This command sends you to the Remote Secret List Configuration mode and the `remote-id-id-type` command. Only one active remote-secret-list is supported per system.

```plaintext
configure

crypto remote-secret-list listname
```

**crypto whitelist file**

Configures a whitelist (access permitted) file to be used by a security gateway (SeGW).

```plaintext
configure

crypto whitelist file pathname
```

**Context Configuration Mode – crypto map**
The following Context Configuration Mode commands have been added in support of IPSec Common Features in a crypto map.

**allow-cert-enc cert-hash-url**

Enables hash and URL encoding in a crypto map.

```
configure
  context <ctxt_name>
    crypto map template_name { ikev2-ipv4 | ikev2-ipv6 }
      allow-cert-enc cert-hash-url
```

**blacklist**

Enables blacklisting in a crypto map.

```
configure
  context <ctxt_name>
    crypto map template_name { ikev2-ipv4 | ikev2-ipv6 }
      blacklist
```

**ocsp**

Enables Online Certificate Status Protocol (OCSP) in a crypto map.

```
configure
  context <ctxt_name>
    crypto map template_name { ikev2-ipv4 | ikev2-ipv6 }
      ocsp [ nonce ]
```

**remote-secret-list**

Enables a remote secret list in a crypto map.

```
configure
  context <ctxt_name>
    crypto map template_name { ikev2-ipv4 | ikev2-ipv6 }
      remote-secret-list
```

**whitelist**

Enables whitelisting in a crypto map.

```
configure
  context <ctxt_name>
    crypto map template_name { ikev2-ipv4 | ikev2-ipv6 }
      whitelist
```
configure

context <ctxt_name>

crypto map template_name { ikev2-ipv4 | ikev2-ipv6 }

whitelist

Context Configuration Mode – crypto template

The following Context Configuration Mode commands have been added in support of IPSec Common Features in a crypto template.

allow-cert-enc cert-hash-url

Enables hash and URL encoding in a crypto template.

configure

context <ctxt_name>

crypto template template_name ikev2-dynamic

   allow-cert-enc cert-hash-url

blacklist

Enables blacklisting in a crypto template.

configure

context <ctxt_name>

crypto template template_name ikev2-dynamic

   blacklist

identity local

Configures the identity of the local IPSec Client (IKE ID).

configure

context <ctxt_name>

crypto template template_name ikev2-dynamic

   identity local id-type type id name

   type configures the IKE identity that the local client uses when authenticating to the gateway. Valid values are:
   • der-ans1-dn: configures NAI Type DER_ASN1_DN (Distinguished Encoding Rules, ASN.1 encoding, Distinguished Name)
   • fqdn: configures NAI Type ID_FQDN (Internet Fully Qualified Domain Name).
- **ip-addr**: configures NAI Type ID_IP_ADDR (IP Address).
- **key-id**: configures NAI Type ID_KEY_ID (opaque octet string).
- **rfc822-addr**: configures NAI Type ID_RFC822_ADDR (RFC 822 email address).

**ocsp**

Enables Online Certificate Status Protocol (OCSP) in a crypto template.

```plaintext
configure
cryptotemplate template_name ikev2-dynamic
ocsp [ nonce ]
```

**remote-secret-list**

Enables a remote secret list in a crypto template.

```plaintext
configure
cryptotemplate template_name ikev2-dynamic
remote-secret-list
```

**whitelist**

Enables whitelisting in a crypto template.

```plaintext
configure
cryptotemplate template_name ikev2-dynamic
whitelist
```

**show Commands**

The following Exec Mode **show** commands have been added in support of IPSec Common Features.

**show cmp history**

Displays historical information for the last 100 Certificate Management Protocol v2 transactions.

```plaintext
show cmp history
```

**show cmp outstanding-req**

show cmp outstanding-req

show cmp statistics

clear Commands
  The following Exec Mode clear commands have been added in support of IPSec Common Features.

clear cmp cert-name
  Clears information stored for the specified IPSec Certificate Management Protocol v2 (CMPv2) certificate.

clear cmp cert-name cert_name

clear cmp statistics

clear cmp statistics

Modified System Security Commands
  This section identifies system security commands modified in release 15.0.

Context Configuration Mode – crypto map
  The following crypto map command has been modified to accommodate IPSec Common Features.

authentication
  Configures the subscriber authentication method used for this crypto map.

configure
  context <ctxt_name>
    crypto map template_name { ikev2-ipv4 | ikev2-ipv6 } authentication { local | remote } { certificate | pre-shared-key { encrypted key value | key value }

Global Configuration Mode

Important: This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

The wsg-service keyword has been added to the congestion-control policy command. This keyword enables congestion control for Wireless Service Gateway service.
configure

  congestion-control policy wsg-service action { drop | none | reject }

Context Configuration Mode – crypto template

The following crypto template command has been modified to accommodate IPSec Common Features.

authentication

Configuration options for the subscriber authentication method used for this crypto template now includes pre-shared keys.

configure

  context <ctxt_name>

    crypto template template_name ikev2-dynamic

    authentication { local | remote } pre-shared key { encrypted key value | key clear_text }

show Commands

The outputs of the following Exec Mode show commands have been modified in support of IPSec Common Features.

show crypto ikev2-ikesa security-associations

Displays a summary view of Internet Key Exchange v2 (IKEv2) IKE Security Associations (IKE SAs).

show crypto ikev2-ikesa security-associations [ peer ipv4/v6_address | summary [ cookies | distribution | dpd | ipsecmgr { instance } | natt [ remote-gw ] ] | tag tag_name ] | [ [ grep grep_options | more ] ]

show crypto ipsec security-associations

Displays IPSec security associations (SAs) configured within or facilitated by the context and can optionally display statistics for them.

show crypto ipsec security-associations [ map-type { ikev2-ipv4-cfg | ikev2-ipv4-node | ikev2-ipv6-cfg | ikev2-ipv6-node | ipsec-dynamic | ipsec-ikev1 | ipsec-ikev2-subscriber | ipsec-l2tp | ipsec-manual | ipsec-mobile-ip } | summary [ distribution | ipsecmgr | map-type ] ] | [ [ grep grep_options | more ] ] | [ tag tag_name ] | [ [ grep grep_options | more ] ]

show crypto statistics

Displays Internet Protocol Security (IPSec) statistics.

show crypto statistics [ ikev1 | ikev2 [ service-ip-address ip-address ] [ service-name name ] | srtcp [ service-ip-address ip-address ] [ service-name name ] ] | [ [ grep grep_options | more ] ]

show crypto template
Displays information about crypto templates.

```
show crypto template [ map-type [ ikev2-dynamic | ipsec-dynamic ] | summary | tag
map_name ] [ | { grep grep_options | more }
```

**Deprecated System Security Commands**

This section identifies system security commands that are no longer supported in release 15.0.

None for this release.
This chapter identifies features and functionality added to, modified for, or deprecated from 15.0 Web Element Manager (WEM) software releases.

**Important:** All functionality from Limited Availability Release StarOS Version 14.1 has been included in General Availability Release StarOS Version 15.0. The Cisco ASR 5x00 Release Change Reference, Version 14.1, details new feature descriptions and configuration, performance, and security changes for the 14.1 release.

**Important:** Enhancements to Diameter, GTPP, and RADIUS in release 15.0 are located in the Accounting Management Changes chapter. Enhancements to SNMP MIBs in release 15.0 are located in the SNMP MIB Changes chapter.
WEM Enhancements for April 30, 2014

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

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

**CSCul68311 - EMS support required new counter "Paging Dropped" in MME S1AP Statistics**

**Feature Changes**

**WEM Support for New MME Counter and Bulkstat**

A new MME counter and a corresponding bulk stat keyword "s1ap-transdata-pagindrop" has been added to the "show mme-service statistics" on ASR5x00. WEM support for this new counter has been added in this feature.

**CSCul68315 - EMS support required for newly added Intra-SRNS and Inter-SRNS bulk-stat**

**Feature Changes**

**WEM Support for Intra-SRNS and Inter-SRNS bulk-stat**

WEM now supports newly added SGSN bulk stats counters for SRNS.

**Performance Indicator Changes**

**SGSN Schema**

The following SGSN counters are now supported on WEM.

- total_att_intra_sgsn_srns
- att_intra_sgsn_ue_involved
- att_intra_sgsn_ue_not_involved
- total_att_inter_sgsn_srns
- att_old_sgsn_inter_sgsn_ue_involved
- att_old_sgsn_inter_srns_ue_not_involved
- att_new_sgsn_inter_srns_ue_involved
- att_new_sgsn_inter_srns_ue_not_involved
- att_old_sgsn_inter_srns_with_mme_ue_involved
- att_old_sgsn_inter_srns_with_mme_ue_not_involved
- att_new_sgsn_inter_srns_with_mme_ue_involved
- att_new_sgsn_inter_srns_with_mme_ue_not_involved

SGSN Schema

The following SGSN counters are now supported on WEM.
- total_suc_intra_sgsn_srns
- suc_intra_srns_ue_involved
- suc_intra_srns_ue_not_involved
- total_suc_inter_sgsn_srns
- suc_old_sgsn_inter_srns_ue_involved
- suc_old_sgsn_inter_srns_ue_not_involved
- suc_new_sgsn_inter_srns_ue_involved
- suc_new_sgsn_inter_srns_ue_not_involved
- suc_old_sgsn_inter_srns_with_mme_ue_involved
- suc_old_sgsn_inter_srns_with_mme_ue_not_involved
- suc_new_sgsn_inter_srns_with_mme_ue_involved
- suc_new_sgsn_inter_srns_with_mme_ue_not_involved

CSCum20624 - EMS support required for the new bulkstats added for CSCui71700

Feature Changes

WEM Support for SGSN Schema

WEM now supports the newly added SGSN counters.

Performance Indicator Changes

SGSN Schema

The following SGSN counters are now supported on WEM.
- redir-attach-rej-gprs-nf
• redir-attach-rej-comb-nf
• redir-periodic-rau-nf_
• redir-rau-gprs-intra-sgsn-rej-nf
• redir-rau-comb-intra-sgsn-rej-nf
• redir-rau-gprs-inter-sgsn-rej-nf
• redir-rau-comb-inter-sgsn-rej-nf
• redir-rau-gprs-inter-rat-nf
• redir-rau-comb-inter-rat-nf
• redir-rau-gprs-inter-serv-nf
• redir-rau-comb-inter-serv-nf
• 2g-attach-redir-ind-nw-failure
• 2g-rau-redir-ind-nw-failure

CSCum26182 - WEM Support for Iurh F2F feature for HNBGW

Feature Changes

WEM Support for F2F Feature

WEM now supports the newly added counters for the following schemas:
• hnbw-hnbap
• hnbw-hnbap-access-closed
• hnbw-hnbap-access-hybrid
• hnbw-hnbap-access-open

Performance Indicator Changes

hnbw-hnbap Schema

WEM now supports the following counters in the hnbw-hnbap schema.
• %ue-dereg-tx-ue-relocated%
• %tnl-update-req-rx%
• %tnl-update-req-rx-cause-reloc-prep%
• %tnl-update-rsp-tx%
• %tnl-update-fail-tx%
• %tnl-update-fail-tx-overload%
• %tnl-update-fail-tx-ue-not-allowed-on-this-hnb%
Web Element Manager Changes in Release 15.0

WEM Enhancements for April 30, 2014

Cisco ASR 5x00 Release Change Reference

- %tnl-update-fail-tx-ml-unspecified%
- %tnl-update-fail-tx-trans-res-unavailable%
- %tnl-update-fail-tx-prot-unspecified%
- %tnl-update-fail-tx-prot-semantic-err%
- %tnl-update-fail-tx-misc-unspecified%
- %reloc-complete-rx%

**hnbgw-hnbap-access-closed Schema**

WEM now supports the following counters in the hnbgw-hnbap-access-closed schema.

- %ue-dereg-tx-ue-relocated%
- %tnl-update-req-rx%
- %tnl-update-req-rx-cause-reloc-prep%
- %tnl-update-rsp-tx%
- %tnl-update-fail-tx%
- %tnl-update-fail-tx-overload%
- %tnl-update-fail-tx-ue-not-allowed-on-this-hnb%
- %tnl-update-fail-tx-ml-unspecified%
- %tnl-update-fail-tx-trans-res-unavailable%
- %tnl-update-fail-tx-prot-unspecified%
- %tnl-update-fail-tx-prot-semantic-err%
- %tnl-update-fail-tx-misc-unspecified%
- %reloc-complete-rx%

**hnbgw-hnbap-access-hybrid Schema**

WEM now supports the following counters in the hnbgw-hnbap-access-hybrid schema.

- %ue-dereg-tx-ue-relocated%
- %tnl-update-req-rx%
- %tnl-update-req-rx-cause-reloc-prep%
- %tnl-update-rsp-tx%
- %tnl-update-fail-tx%
- %tnl-update-fail-tx-overload%
- %tnl-update-fail-tx-ue-not-allowed-on-this-hnb%
- %tnl-update-fail-tx-ml-unspecified%
- %tnl-update-fail-tx-trans-res-unavailable%
- %tnl-update-fail-tx-prot-unspecified%
Web Element Manager Changes in Release 15.0

WEM Enhancements for April 30, 2014

- %tnl-update-fail-tx-prot-semantic-err%
- %tnl-update-fail-tx-misc-unspecified%
- %reloc-complete-rx%

### hnbgw-hnbap-access-open Schema

WEM now supports the following counters in the hnbgw-hnbap-access-open schema.

- %ue-dereg-tx-ue-relocated%
- %tnl-update-req-rx%
- %tnl-update-req-rx-cause-reloc-prep%
- %tnl-update-rsp-tx%
- %tnl-update-fail-tx%
- %tnl-update-fail-tx-overload%
- %tnl-update-fail-tx-ue-not-allowed-on-this-hnb%
- %tnl-update-fail-tx-rnl-unspecified%
- %tnl-update-fail-tx-trans-res-unavailable%
- %tnl-update-fail-tx-prot-unspecified%
- %tnl-update-fail-tx-prot-semantic-err%
- %tnl-update-fail-tx-misc-unspecified%
- %reloc-complete-rx%

### CSCum54746 - [BS Config]: "Syst Local File Storage" configurable is removed from CLI

**Feature Changes**

**Removal of “System Local Storage” Field from WEM GUI Screens**

The System Local Storage fields have been removed from Bulk Statistics screen and Bulk Statistics Configuration screen.

### CSCum73297 - [BS] Counters not supported in WEM

**Feature Changes**

**Support for BS Counters on WEM**

The following BS counters are supported on WEM.
Performance Indicator Changes

IPSG Schema

The following counters are supported on WEM.

- total-discard-msgs-partial-match-interim
- total_discard_msgs_partial_match_start

System Schema

The following counters are supported on WEM.

- %disc-reason-534%
- %disc-reason-535%
- %disc-reason-536%
- %disc-reason-537%
- %disc-reason-538%
- %disc-reason-539%
- %disc-reason-540%
- %disc-reason-541%
- %disc-reason-542%
- %disc-reason-543%
- %disc-reason-544%
- %disc-reason-545%
- %disc-reason-546%
- %disc-reason-547%
- %disc-reason-548%
- %disc-reason-549%
- %disc-reason-550%
- %disc-reason-551%
- %disc-reason-552%

CSCum80541 - WEM 15.0.2304 - GUI not showing 15.0 ASR5x00 crash data correctly.

Feature Changes

WEM GUI Displays ASR5x00 Data
The WEM GUI did not display the crash data correctly for ASR5x00’s, which are on a 15.0 software release, although ASR5x00’s software has a 'crash-grouping-feature':

**Previous Behavior:** In 15.0, The WEM GUI did not display the crash data correctly for ASR5x00’s, which are on a 15.0 software release, although ASR5x00’s software has a 'crash-grouping-feature':

**New Behavior:** WEM GUI now displays the crash data correctly for ASR5x00. WEM GUI also displays “Similar Crash Count” and "Time of First Crash".

### CSCun22514 - Bulk statistics support for ASR5K R16

**Feature Changes**

**Bulk Statistics Support**

Bulk statistics support for the following counters has been added in this release.

**Performance Indicator Changes**

**dpca Schema**

The `server-type` filter was added for this schema.

**ippool Schema**

Following filters are added for this schema:

- `addrtype`
- `type`
- `state`
- `priority`

**system Schema**

Following counters are added for this schema:

- `wsg-cursess`
- `wsg-curactive`
- `wsg-curdormant`
- `wsg-ttlsetup`
- `wsg-curchildsa`

**hnbgw_rua_hybrid Schema**

Following counters are added for this schema:

- `cs-connect-tx-est-cause-emergency`
- `cs-connect-tx-est-cause-normal`
- ps-connect-tx-est-cause-emergency
- ps-connect-tx-est-cause-normal

**hnbgw_rua_open Schema**

Following counters are added for this schema:
- cs-connect-tx-est-cause-emergency
- cs-connect-tx-est-cause-normal
- ps-connect-tx-est-cause-emergency
- ps-connect-tx-est-cause-normal

**hnbgw_rua_closed Schema**

Following counters are added for this schema:
- cs-connect-tx-est-cause-emergency
- cs-connect-tx-est-cause-normal
- ps-connect-tx-est-cause-emergency
- ps-connect-tx-est-cause-normal

**imsa Schema**

Following counters are added for this schema:
- dpca-msg-ccainitdrop
- dpca-msg-ccaupddrop
- dpca-msg-ccafindrop
- dpca-msg-ccainitfail
- dpca-msg-ccaupdfail
- dpca-msg-ccafinfail
- dpca-total-ims-auth-fh-triggered
- dpca-imsa-raa-msg-success
- dpca-imsa-raa-msgerr-3xxx
- dpca-imsa-raa-msgerr-4xxx
- dpca-imsa-raa-msgerr-5xxx
- dpca-imsa-raa-msgerr-otherrrcode
- dpca-imsa-bp-ccri-msgs
- dpca-imsa-bp-ccri-msg-failures
- dpca-imsa-bp-ccri-sessid-rcvry-failures
- dpca-imsa-bp-ccru-msgs
- dpca-imsa-bp-ccru-msg-failures
- dpca-imsa-bp-ccru-max-retry_msgs
- dpca-imsa-bp-ccru-dropped-msgs
- dpca-imsa-bp-ccru-sessid-rcvry-failures
- dpca-imsa-bp-ccrt-msgs
- dpca-imsa-bp-ccrt-msg-failures
- dpca-imsa-bp-ccrt-sessid-rcvry-failures

**hnbw_ranap Schema**

Following counters are added for this schema:

- cs-reloc-prep-failure-tx

**hnbw_hnbap Schema**

Following counters are added for this schema:

- ue-dereg-tx-ue-relocated
- tnl-update-req-rx
- tnl-update-req-rx-cause-reloc-prep
- tnl-update-rsp-tx
- tnl-update-fail-tx
- tnl-update-fail-tx-overload
- tnl-update-fail-tx-ue-not-allowed-on-this-hnb
- tnl-update-fail-tx-rnl-unspecified
- tnl-update-fail-tx-trans-res-unavailable
- tnl-update-fail-tx-prot-unspecified
- tnl-update-fail-tx-prot-semantic-err
- tnl-update-fail-tx-misc-unspecified
- reloc-complete-rx

**ecs Schema**

Following counters are added for this schema:

- ip-accel-pkts
- udp-accel-pkts
- tcp-accel-pkts
- http-accel-pkts
- https-accel-pkts

**dpca Schema**
Following counters are added for this schema:

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

**dcca Schema**

Following counters are added for this schema:

- mscc-gsu-null-grant
- mscc-fui-redirect
- cca-2xxx-rc
- ccri-bp-stats
- ccru-bp-stats
- ccrt-bp-stats
- cs_nw_ranap
- reloc-prep-failure-rx

**apn Schema**

Following counters are added for this schema:

- qci1-uplinkpkt-drop-mbrexcd
- qci1-dwlinkpkt-drop-mbrexcd
- qci1-uplinkbyte-drop-mbrexcd
- qci1-dwlinkbyte-drop-mbrexcd
- qci1-rejbearer
- qci2-uplinkpkt-drop-mbrexcd
- qci2-dwlinkpkt-drop-mbrexcd
- qci2-uplinkbyte-drop-mbrexcd
- qci2-dwlinkbyte-drop-mbrexcd
- qci2-rejbearer
- qci3-uplinkpkt-drop-mbrexcd
- qci3-dwlinkpkt-drop-mbrexcd
- qci3-uplinkbyte-drop-mbrexcd
- qci3-dwlinkbyte-drop-mbrexcd
- qci3-rejbearer
- qci4-uplinkpkt-drop-mbrexcd
- qci4-dwlinkpkt-drop-mbrexcd
- qci4-uplinkbyte-drop-mbrexcd
- qci4-dwlinkbyte-drop-mbrexcld
- qci4-rejbearer
- qci5-uplinkpkt-drop-mbrexcld
- qci5-dwlinkpkt-drop-mbrexcld
- qci5-uplinkbyte-drop-mbrexcld
- qci5-dwlinkbyte-drop-mbrexcld
- qci5-rejbearer
- qci6-uplinkpkt-drop-mbrexcld
- qci6-dwlinkpkt-drop-mbrexcld
- qci6-uplinkbyte-drop-mbrexcld
- qci6-dwlinkbyte-drop-mbrexcld
- qci6-rejbearer
- qci7-uplinkpkt-drop-mbrexcld
- qci7-dwlinkpkt-drop-mbrexcld
- qci7-uplinkbyte-drop-mbrexcld
- qci7-dwlinkbyte-drop-mbrexcld
- qci7-rejbearer
- qci8-uplinkpkt-drop-mbrexcld
- qci8-dwlinkpkt-drop-mbrexcld
- qci8-uplinkbyte-drop-mbrexcld
- qci8-dwlinkbyte-drop-mbrexcld
- qci8-rejbearer
- qci9-uplinkpkt-drop-mbrexcld
- qci9-dwlinkpkt-drop-mbrexcld
- qci9-uplinkbyte-drop-mbrexcld
- qci9-dwlinkbyte-drop-mbrexcld
- qci9-rejbearer
- invalidqci-rejbearer

**pgw Schema**

Following counters are added for this schema:
- sessstat-bearerl-nwded4sgsn
- sessstat-bearerl-nores-s6brad-ip
- sessstat-bearerl-nores-ims-auth-failed
- sessstat-bearerl-nores-chrgsvc-auth-failed
• sessstat-bearrej-nores-dhcp-ip-failed
• sessstat-bearrej-nores-setup-timeout
• sessstat-bearrej-nores-aaa-auth-exceed
• sessstat-bearrej-nores-no-sess-aaa
• sessstat-bearrej-nores-conflict-ip-addr
• sessstat-bearrej-nores-static-ip
• sessstat-bearrej-nores-msreq-invalid-ip
• sessstat-bearrej-nores-other-reason
• servstat-upPrioritymark-p0
• servstat-upPrioritymark-p1
• servstat-upPrioritymark-p2
• servstat-upPrioritymark-p3
• servstat-upPrioritymark-p4
• servstat-upPrioritymark-p5
• servstat-upPrioritymark-p6
• servstat-upPrioritymark-p7
• servstat-downPrioritymark-p0
• servstat-downPrioritymark-p1
• servstat-downPrioritymark-p2
• servstat-downPrioritymark-p3
• servstat-downPrioritymark-p4
• servstat-downPrioritymark-p5
• servstat-downPrioritymark-p6
• servstat-downPrioritymark-p7

sgw Schema

Following counters are added for this schema:
• totepsbearrel-dedrsn-pgw-qci1
• totepsbearrel-dedrsn-pgw-qci2
• totepsbearrel-dedrsn-pgw-qci3
• totepsbearrel-dedrsn-pgw-qci4
• totepsbearrel-dedrsn-pgw-qci5
• totepsbearrel-dedrsn-pgw-qci6
• totepsbearrel-dedrsn-pgw-qci7
• totepsbearrel-dedrsn-pgw-qci8
- `totepsbearrel-dedrsn-pgw-qci9`
- `totepsbearrel-dedrsn-pgw-qci-other`
- `totepsbearrel-dedrsn-s1err-qci1`
- `totepsbearrel-dedrsn-s1err-qci2`
- `totepsbearrel-dedrsn-s1err-qci3`
- `totepsbearrel-dedrsn-s1err-qci4`
- `totepsbearrel-dedrsn-s1err-qci5`
- `totepsbearrel-dedrsn-s1err-qci6`
- `totepsbearrel-dedrsn-s1err-qci7`
- `totepsbearrel-dedrsn-s1err-qci8`
- `totepsbearrel-dedrsn-s1err-qci9`
- `totepsbearrel-dedrsn-s1err-qci-other`
- `totepsbearrel-dedrsn-s5err-qci1`
- `totepsbearrel-dedrsn-s5err-qci2`
- `totepsbearrel-dedrsn-s5err-qci3`
- `totepsbearrel-dedrsn-s5err-qci4`
- `totepsbearrel-dedrsn-s5err-qci5`
- `totepsbearrel-dedrsn-s5err-qci6`
- `totepsbearrel-dedrsn-s5err-qci7`
- `totepsbearrel-dedrsn-s5err-qci8`
- `totepsbearrel-dedrsn-s5err-qci9`
- `totepsbearrel-dedrsn-s5err-qci-other`
- `totepsbearrel-dedrsn-s4err-qci1`
- `totepsbearrel-dedrsn-s4err-qci2`
- `totepsbearrel-dedrsn-s4err-qci3`
- `totepsbearrel-dedrsn-s4err-qci4`
- `totepsbearrel-dedrsn-s4err-qci5`
- `totepsbearrel-dedrsn-s4err-qci6`
- `totepsbearrel-dedrsn-s4err-qci7`
- `totepsbearrel-dedrsn-s4err-qci8`
- `totepsbearrel-dedrsn-s4err-qci9`
- `totepsbearrel-dedrsn-s4err-qci-other`
- `totepsbearrel-dedrsn-s12err-qci1`
- `totepsbearrel-dedrsn-s12err-qci2`
- totepsbearrel-dedrsn-s12err-qci3
- totepsbearrel-dedrsn-s12err-qci4
- totepsbearrel-dedrsn-s12err-qci5
- totepsbearrel-dedrsn-s12err-qci6
- totepsbearrel-dedrsn-s12err-qci7
- totepsbearrel-dedrsn-s12err-qci8
- totepsbearrel-dedrsn-s12err-qci9
- totepsbearrel-dedrsn-s12err-qci-other
- totepsbearrel-dedrsn-local-qci1
- totepsbearrel-dedrsn-local-qci2
- totepsbearrel-dedrsn-local-qci3
- totepsbearrel-dedrsn-local-qci4
- totepsbearrel-dedrsn-local-qci5
- totepsbearrel-dedrsn-local-qci6
- totepsbearrel-dedrsn-local-qci7
- totepsbearrel-dedrsn-local-qci8
- totepsbearrel-dedrsn-local-qci9
- totepsbearrel-dedrsn-local-qci-other
- totepsbearrel-dedrsn-pdn-qci1
- totepsbearrel-dedrsn-pdn-qci2
- totepsbearrel-dedrsn-pdn-qci3
- totepsbearrel-dedrsn-pdn-qci4
- totepsbearrel-dedrsn-pdn-qci5
- totepsbearrel-dedrsn-pdn-qci6
- totepsbearrel-dedrsn-pdn-qci7
- totepsbearrel-dedrsn-pdn-qci8
- totepsbearrel-dedrsn-pdn-qci9
- totepsbearrel-dedrsn-pdn-qci-other
- totepsbearrel-dedrsn-pathfail-s1-u-qci1
- totepsbearrel-dedrsn-pathfail-s1-u-qci2
- totepsbearrel-dedrsn-pathfail-s1-u-qci3
- totepsbearrel-dedrsn-pathfail-s1-u-qci4
- totepsbearrel-dedrsn-pathfail-s1-u-qci5
- totepsbearrel-dedrsn-pathfail-s1-u-qci6
- totpsbearrel-dedrsn-pathfail-s1-u-qci7
- totpsbearrel-dedrsn-pathfail-s1-u-qci8
- totpsbearrel-dedrsn-pathfail-s1-u-qci9
- totpsbearrel-dedrsn-pathfail-s1-u-qci-other
- totpsbearrel-dedrsn-pathfail-s5-u-qci1
- totpsbearrel-dedrsn-pathfail-s5-u-qci2
- totpsbearrel-dedrsn-pathfail-s5-u-qci3
- totpsbearrel-dedrsn-pathfail-s5-u-qci4
- totpsbearrel-dedrsn-pathfail-s5-u-qci5
- totpsbearrel-dedrsn-pathfail-s5-u-qci6
- totpsbearrel-dedrsn-pathfail-s5-u-qci7
- totpsbearrel-dedrsn-pathfail-s5-u-qci8
- totpsbearrel-dedrsn-pathfail-s5-u-qci9
- totpsbearrel-dedrsn-pathfail-s5-u-qci-other
- totpsbearrel-dedrsn-pathfail-s5-qci1
- totpsbearrel-dedrsn-pathfail-s5-qci2
- totpsbearrel-dedrsn-pathfail-s5-qci3
- totpsbearrel-dedrsn-pathfail-s5-qci4
- totpsbearrel-dedrsn-pathfail-s5-qci5
- totpsbearrel-dedrsn-pathfail-s5-qci6
- totpsbearrel-dedrsn-pathfail-s5-qci7
- totpsbearrel-dedrsn-pathfail-s5-qci8
- totpsbearrel-dedrsn-pathfail-s5-qci9
- totpsbearrel-dedrsn-pathfail-s5-qci-other
- totpsbearrel-dedrsn-pathfail-s11
- totpsbearrel-dedrsn-pathfail-s11-qci1
- totpsbearrel-dedrsn-pathfail-s11-qci2
- totpsbearrel-dedrsn-pathfail-s11-qci3
- totpsbearrel-dedrsn-pathfail-s11-qci4
- totpsbearrel-dedrsn-pathfail-s11-qci5
- totpsbearrel-dedrsn-pathfail-s11-qci6
- totpsbearrel-dedrsn-pathfail-s11-qci7
- totpsbearrel-dedrsn-pathfail-s11-qci8
- totpsbearrel-dedrsn-pathfail-s11-qci9
- totepsbearrel-dedrsn-pathfail-s11-qci-other
- totepsbearrel-dedrsn-pathfail-s12-qci1
- totepsbearrel-dedrsn-pathfail-s12-qci2
- totepsbearrel-dedrsn-pathfail-s12-qci3
- totepsbearrel-dedrsn-pathfail-s12-qci4
- totepsbearrel-dedrsn-pathfail-s12-qci5
- totepsbearrel-dedrsn-pathfail-s12-qci6
- totepsbearrel-dedrsn-pathfail-s12-qci7
- totepsbearrel-dedrsn-pathfail-s12-qci8
- totepsbearrel-dedrsn-pathfail-s12-qci9
- totepsbearrel-dedrsn-pathfail-s12-qci-other
- totepsbearrel-dedrsn-pathfail-s4-u-qci1
- totepsbearrel-dedrsn-pathfail-s4-u-qci2
- totepsbearrel-dedrsn-pathfail-s4-u-qci3
- totepsbearrel-dedrsn-pathfail-s4-u-qci4
- totepsbearrel-dedrsn-pathfail-s4-u-qci5
- totepsbearrel-dedrsn-pathfail-s4-u-qci6
- totepsbearrel-dedrsn-pathfail-s4-u-qci7
- totepsbearrel-dedrsn-pathfail-s4-u-qci8
- totepsbearrel-dedrsn-pathfail-s4-u-qci9
- totepsbearrel-dedrsn-pathfail-s4-u-qci-other
- totepsbearrel-dedrsn-inactivity-timeout
- totepsbearrel-dedrsn-inactivity-timeout-qci1
- totepsbearrel-dedrsn-inactivity-timeout-qci2
- totepsbearrel-dedrsn-inactivity-timeout-qci3
- totepsbearrel-dedrsn-inactivity-timeout-qci4
- totepsbearrel-dedrsn-inactivity-timeout-qci5
- totepsbearrel-dedrsn-inactivity-timeout-qci6
- totepsbearrel-dedrsn-inactivity-timeout-qci7
- totepsbearrel-dedrsn-inactivity-timeout-qci8
- totepsbearrel-dedrsn-inactivity-timeout-qci9
- totepsbearrel-dedrsn-inactivity-timeout-qci-other
SGSN Schema

Following counters are added for this schema:

- totepsbearrel-dedrsn-other-qci3
- totepsbearrel-dedrsn-other-qci4
- totepsbearrel-dedrsn-other-qci5
- totepsbearrel-dedrsn-other-qci6
- totepsbearrel-dedrsn-other-qci7
- totepsbearrel-dedrsn-other-qci8
- totepsbearrel-dedrsn-other-qci9
- totepsbearrel-dedrsn-other-qci-other
- lcl-cleanup-bearer-not-in-same-state
- lcl-cleanup-bearer-not-in-correct-state
- lcl-cleanup-dup-data-teid
- lcl-cleanup-remote-addr-not-compatible
- lcl-cleanup-bad-peer
- lcl-cleanup-bearer-ctxt-missing

**SGSN Schema**

Following counters are added for this schema:

- 3G-attach-rej-network-failure-no-data-from-hlr
- 3G-attach-rej-network-failure-congestion-thrtl
- 3G-attach-rej-network-failure-opr-policy-failure
- 3G-attach-rej-network-failure-check-imei-timeout-eir
- 3G-attach-rej-network-failure-rnc-ovld
- 3G-attach-rej-network-failure-more-ius-same-imsi
- 3G-attach-rej-network-failure-no-resource-intl-failure
- 2G-attach-rej-network-failure-no-data-from-hlr
- 2G-attach-rej-network-failure-congestion-thrtl
- 2G-attach-rej-network-failure-opr-policy-failure
- 2G-attach-rej-network-failure-check-imei-timeout-eir
- 3G-comb-attach-rej-network-failure-no-data-from-hlr
- 3G-comb-attach-rej-network-failure-congestion-thrtl
- 3G-comb-attach-rej-network-failure-opr-policy-failure
- 3G-comb-attach-rej-network-failure-check-imei-timeout-eir
- 3G-comb-attach-rej-network-failure-rnc-ovld
- 3G-comb-attach-rej-network-failure-more-ius-same-imsi
- 3G-comb-attach-rej-network-failure-no-resource-intl-failure
- 2G-comb-attach-rej-network-failure-no-data-from-hlr
- 2G-comb-attach-rej-network-failure-congestion-thrtl
- 2G-comb-attach-rej-network-failure-opr-policy-failure
- 2G-comb-attach-rej-network-failure-check-imei-timeout-eir
- total_att_intra_sgsn_srns
- att_intra_srns_ue_involved
- att_intra_srns_ue_not_involved
- total_att_inter_sgsn_srns
- att_old_sgsn_inter_srns_ue_involved
- att_old_sgsn_inter_srns_ue_not_involved
- att_new_sgsn_inter_srns_ue_involved
- att_new_sgsn_inter_srns_ue_not_involved
- att_old_sgsn_inter_srns_with_mme_ue_involved
- att_old_sgsn_inter_srns_with_mme_ue_not_involved
- att_new_sgsn_inter_srns_with_mme_ue_involved
- att_new_sgsn_inter_srns_with_mme_ue_not_involved
- total_suc_intra_sgsn_srns
- suc_intra_srns_ue_involved
- suc_intra_srns_ue_not_involved
- total_suc_inter_sgsn_srns
- suc_old_sgsn_inter_srns_ue_involved
- suc_old_sgsn_inter_srns_ue_not_involved
- suc_new_sgsn_inter_srns_ue_involved
- suc_new_sgsn_inter_srns_ue_not_involved
- suc_old_sgsn_inter_srns_with_mme_ue_involved
- suc_old_sgsn_inter_srns_with_mme_ue_not_involved
- suc_new_sgsn_inter_srns_with_mme_ue_involved
- suc_new_sgsn_inter_srns_with_mme_ue_not_involved
- redir-attach-rej-gprs-ncil
- redir-attach-rej-comb-ncil
- redir-periodic-rau-ncil
- redir-rau-gprs-intra-sgsn-rej-ncil
- redir-rau-comb-intra-sgsn-rej-ncil
- redir-rau-gprs-inter-sgsn-rej-ncil
- `redir-rau-comb-inter-sgsn-rej-ncil`
- `redir-rau-gprs-inter-rat-ncil`
- `redir-rau-comb-inter-rat-ncil`
- `redir-rau-gprs-inter-serv-ncil`
- `redir-rau-comb-inter-serv-ncil`
- `redir-attach-rej-gprs-nf`
- `redir-attach-rej-comb-nf`
- `redir-periodic-rau-nf`
- `redir-rau-gprs-intra-sgsn-rej-nf`
- `redir-rau-comb-intra-sgsn-rej-nf`
- `redir-rau-gprs-inter-sgsn-rej-nf`
- `redir-rau-comb-inter-sgsn-rej-nf`
- `redir-rau-gprs-inter-rat-nf`
- `redir-rau-comb-inter-rat-nf`
- `redir-rau-gprs-inter-serv-nf`
- `redir-rau-comb-inter-serv-nf`
- `2g-total-attach-redir-attempt`
- `2g-attach-req-redir-attempt-with-imsi`
- `2g-attach-req-redir-attempt-without-imsi`
- `2g-total-attach-redir-comp`
- `2g-attach-redir-comp-success`
- `2g-attach-redir-comp-failure`
- `2g-attach-redir-indication`
- `2g-attach-redir-ind-ill-plmn`
- `2g-attach-redir-ind-ill-la`
- `2g-attach-redir-ind-no-roam`
- `2g-attach-redir-ind-no-gprs-plmn`
- `2g-attach-redir-ind-no-cell-in-la`
- `2g-attach-redir-ind-csp-cert-la`
- `2g-attach-redir-ind-nw-failure`
- `2g-attach-redir-ind-others`
- `2g-total-rau-redir-attempt`
- `2g-rau-req-redir-attempt-with-imsi`
- `2g-rau-req-redir-attempt-without-imsi`
- 2g-total-rau-redir-comp
- 2g-rau-redir-comp-success
- 2g-rau-redir-comp-failure
- 2g-rau-redir-indication
- 2g-rau-redir-ind-ill-plmn
- 2g-rau-redir-ind-ill-la
- 2g-rau-redir-ind-no-roam
- 2g-rau-redir-ind-no-gprs-plmn
- 2g-rau-redir-ind-no-cell-in-la
- 2g-rau-redir-ind-csps-req
- 2g-rau-redir-ind-nw-failure
- 2g-rau-redir-ind-others
- common-ra-3g-page-req同same-rat
- common-ra-2g-page-req同same-rat
- common-ra-3g-page-req-ret同same-rat
- common-ra-2g-page-req-ret同same-rat
- common-ra-3g-page-req-oth-oth-rat
- common-ra-2g-page-req-oth-oth-rat
- common-ra-3g-page-req-ret-oth-rat
- common-ra-2g-page-req-ret-oth-rat
- common-ra-3g-page-rsp同same-rat
- common-ra-2g-page-rsp同same-rat
- common-ra-3g-page-rsp-att-oth-rat
- common-ra-2g-page-rsp-att-oth-rat
- common-ra-3g-page-rsp-rau-oth-rat
- common-ra-2g-page-rsp-rau-oth-rat
- common-ra-3g-page-rsp-power-off-oth-rat
- common-ra-2g-page-rsp-power-off-oth-rat
- common-ra-3g-page-timeout-oth-rat
- common-ra-2g-page-timeout-oth-rat
- common-ra-3g-page-stop
- common-ra-2g-page-stop
- common-ra-3g-attach-oth-rat
- common-ra-2g-attach-oth-rat
mme Schema

Following counters are added for this schema:

- s1ap-transdata-pagingdrop
- ps-qci-1-paging-init-events-attempted
- ps-qci-1-paging-init-events-success
- ps-qci-1-paging-init-events-failures
- ps-qci-1-paging-last-enb-success
- ps-qci-1-paging-last-tai-success
- ps-qci-1-paging-tai-list-success
- ps-qci-2-paging-init-events-attempted
- ps-qci-2-paging-init-events-success
- ps-qci-2-paging-init-events-failures
- ps-qci-2-paging-last-enb-success
- ps-qci-2-paging-last-tai-success
- ps-qci-2-paging-tai-list-success
- ps-qci-3-paging-init-events-attempted
- ps-qci-3-paging-init-events-success
- ps-qci-3-paging-init-events-failures
- ps-qci-3-paging-last-enb-success
- ps-qci-3-paging-last-tai-success
- ps-qci-3-paging-tai-list-success
- ps-qci-4-paging-init-events-attempted
- ps-qci-4-paging-init-events-success
- ps-qci-4-paging-init-events-failures
- ps-qci-4-paging-last-enb-success
- ps-qci-4-paging-last-tai-success
- ps-qci-4-paging-tai-list-success
- ps-qci-5-paging-init-events-attempted
- ps-qci-5-paging-init-events-success
- ps-qci-5-paging-init-events-failures
- ps-qci-5-paging-last-enb-success
- ps-qci-5-paging-last-tai-success
- ps-qci-5-paging-tai-list-success
- ps-qci-6-paging-init-events-attempted
- ps-qci-6-paging-init-events-success
- ps-qci-6-paging-init-events-failures
- ps-qci-6-paging-last-enb-success
- ps-qci-6-paging-last-tai-success
- ps-qci-6-paging-tai-list-success
- ps-qci-7-paging-init-events-attempted
- ps-qci-7-paging-init-events-success
- ps-qci-7-paging-init-events-failures
- ps-qci-7-paging-last-enb-success
- ps-qci-7-paging-last-tai-success
- ps-qci-7-paging-tai-list-success
- ps-qci-8-paging-init-events-attempted
- ps-qci-8-paging-init-events-success
- ps-qci-8-paging-init-events-failures
- ps-qci-8-paging-last-enb-success
- ps-qci-8-paging-last-tai-success
- ps-qci-8-paging-tai-list-success
- ps-qci-9-paging-init-events-attempted
- ps-qci-9-paging-init-events-success
- ps-qci-9-paging-init-events-failures
- ps-qci-9-paging-last-enb-success
- ps-qci-9-paging-last-tai-success
- ps-qci-9-paging-tai-list-success
- signaling-detach-paging-init-events-attempted
- signaling-detach-paging-init-events-success
- signaling-detach-paging-init-events-failures
- signaling-detach-paging-last-enb-success
- signaling-detach-paging-last-tai-success
- signaling-detach-paging-tai-list-success
- signaling-lcs-paging-init-events-attempted
- signaling_lcs-paging-init-events-success
- signaling-lcs-paging-init-events-failures
- signaling-lcs-paging-last-enb-success
- signaling-lcs-paging-last-tai-success
- signaling-lcs-paging-tai-list-success
- emm-msgtx-attach-rej-opr-determined-barring
- emm-msgtx-attach-rej-insuff-resources
- emm-msgtx-attach-rej-activation-reject
- emm-msgtx-attach-rej-svc-temp-out-of-order
- emm-msgtx-attach-rej-protocol-error
- emm-msgtx-attach-rej-apn-restrict-incompatible
- emm-msgtx-tau-inter-accept
- emm-msgtx-tau-inter-accept-retx
- emm-msgtx-tau-inter-accept-imsi-unknown
- emm-msgtx-tau-inter-accept-no-msc
- emm-msgtx-tau-inter-accept-nw-fail
- emm-msgtx-tau-inter-accept-congestion
- emm-msgtx-tau-inter-accept-no-cs
- emm-msgtx-tau-intra-accept
- emm-msgtx-tau-intra-accept-retx
- emm-msgtx-tau-intra-accept-imsi-unknown
- emm-msgtx-tau-intra-accept-no-msc
- emm-msgtx-tau-intra-accept-nw-fail
- emm-msgtx-tau-intra-accept-congestion
- emm-msgtx-tau-intra-accept-no-cs
- emm-msgtx-tau-csg-not-subscribed
- emm-msgtx-tau-eps-non-eps-not-allowed
- emm-msgtx-tau-inter-reject
- emm-msgtx-tau-inter-imsi-unknown-hss
- emm-msgtx-tau-inter-illegal-ue
- emm-msgtx-tau-inter-illegal-me
- emm-msgtx-tau-inter-eps-not-allowed
- emm-msgtx-tau-inter-network-fail
- emm-msgtx-tau-inter-decode-failure
- emm-msgtx-tau-inter-no-bearer-active
- emm-msgtx-tau-inter-ue-identity-unk
- emm-msgtx-tau-inter-implicit-detached
- emm-msgtx-tau-inter-imei-not-accept
- emm-msgtx-tau-inter-roaming-restrict-ta
- emm-msgtx-tau-inter-plmn-not-allow
- emm-msgtx-tau-inter-no-suitable-cell-ta
- emm-msgtx-tau-inter-ta-not-allow
- emm-msgtx-tau-inter-no-eps-svc-plmn
- emm-msgtx-tau-inter-csg-not-subscribed
- emm-msgtx-tau-inter-eps-non-eps-not-allowed
- emm-msgtx-tau-intra-reject
- emm-msgtx-tau-intra-imsi-unknown-hss
- emm-msgtx-tau-intra-illegal-ue
- emm-msgtx-tau-intra-illegal-me
- emm-msgtx-tau-intra-eps-not-allowed
- emm-msgtx-tau-intra-network-fail
- emm-msgtx-tau-intra-decode-failure
- emm-msgtx-tau-intra-no-bearer-active
- emm-msgtx-tau-intra-ue-identity-unk
- emm-msgtx-tau-intra-implicit-detached
- emm-msgtx-tau-intra-imei-not-accept
- emm-msgtx-tau-intra-roaming-restrict-ta
- emm-msgtx-tau-intra-plmn-not-allow
- emm-msgtx-tau-intra-no-suitable-cell-ta
- emm-msgtx-tau-intra-ta-not-allow
- emm-msgtx-tau-intra-no-eps-svc-plmn
- emm-msgtx-tau-intra-csg-not-subscribed
- emm-msgtx-tau-intra-eps-non-eps-not-allowed
- emmsgtx-tau-inter-req
- emmsgtx-tau-inter-retx
- emmsgtx-tau-intra-req
- emmsgtx-tau-intra-retx
- esm-msgtx-pdncon-rej-opr-determined-barring
- esm-msgtx-pdncon-rej-insuff-resources
- esm-msgtx-pdncon-rej-activation-reject
- esm-msgtx-pdncon-rej-svc-temp-out-of-order
- esm-msgtx-pdncon-rej-protocol-errors
- esm-msgtx-pdncon-rej-apn-restrict-incompatible
- out-non-3GPP-ho-attempted
- out-non-3GPP-ho-success
- out-non-3GPP-ho-failures
- in-non-3GPP-ho-attempted
- in-non-3GPP-ho-success
- in-non-3GPP-ho-failures

**dcca_group Schema**

Following counters are added for this schema:

- msc-gsu-null-grant
- msc-fui-redirect
- cca-2xxx-rc
- ccri-bp-stats
- ccru-bp-stats
- ccrt-bp-stats

**epdg Schema**

Following counters are added for this schema:

- num-qci1_bearer_active
- num-qci1_bearer_setup
- num-qci1_bearer_released
- num-qci2_bearer_active
- num-qci2_bearer_setup
- num-qci2_bearer_released
- num-qci3_bearer_active
- num-qci3_bearer_setup
- num-qci3_bearer_released
- num-qci4_bearer_active
- num-qci4_bearer_setup
- num-qci4_bearer_released
• num-qci5_bearer_active
• num-qci5_bearer_setup
• num-qci5_bearer_released
• num-qci6_bearer_active
• num-qci6_bearer_setup
• num-qci6_bearer_released
• num-qci7_bearer_active
• num-qci7_bearer_setup
• num-qci7_bearer_released
• num-qci8_bearer_active
• num-qci8_bearer_setup
• num-qci8_bearer_released
• num-qci9_bearer_active
• num-qci9_bearer_setup
• num-qci9_bearer_released
• totgtp-curr-ue-in-sys
• num-disc-invalid-pdn-type

CSCun24706 - Alarm support for ASR5K R16

Feature Changes

Alarm Support for ASR5x00

In this release, the following alarms have been supported:

• starHENBGMESCTPAassocDestAddrDown
• starHENBGMESCTPAassocDestAddrUp
• starMRMEServiceStart
• starMRMEServiceStop
• starThreshPerServiceSAMOGSessions
• starThreshClearPerServiceSAMOGSessions
WEM Enhancements for Jan 31, 2014

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

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

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

---

**CSCue70505 - Add PCF as an Index in PPP and RP Schemas**

**Feature Changes**

**Add PCF as an Index in PPP and RP Schemas**

WEM now supports PCF as an index in PPP and RP schemas.

**Previous Behavior:** WEM did not support PPP Per PCF Schema and PPP Per RP Schema.

**New Behavior:** WEM now supports PPP Per PCF Schema and PPP Per RP Schema was not supported.

**Customer Impact:**

---

**Performance Indicator Changes**

**PPP Per PCF Schema**
Added ppp-per-pcf schema support in WEM.
- vpnname
- vpnid
- servname
- servid
- pcf-ip-addr
- recv-total
- accept-total
- update-total
- update-ack-recv-total

PPP Per RP Schema

Added ppp-per-rp schema support in WEM.
- vpnname
- vpnid
- servname
- servid
- pcf-ip-addr
- total-init
- total-sess-succ
- total-sess-succ
- total-auth
- total-ipcp

CSCui90658 - KT EPC : SGW - UDPC : Support required for UDPC UMIO and DPC(R02) in WEM

Feature Changes

Support added for UDPC, UMIO, and DPC2 Cards

Support for UDPC, UMIO, and DPC2 cards have been added in WEM. The card support is available in the following screens:

In System Info menu:
- Rear View — UDPC and UMIO card images are displayed on this screen.
- CPU Information — UDPC and UMIO cards CPU Information is listed in the table and graph support has been provided for them.
- Port Information — UMIO cards port information details are listed in the table on this screen.

In Accounting menu:
- View/Graph Bulk Statistics — UDPC and UMIO cards bulk statistics graph support is added on this screen after selecting card in the combo box.

CSCuj14134 - Support required for new BS counters in 15.0

Feature Changes

New BS Counters Supported on WEM

New BS counters that were available on ASR5k are now supported on WEM.

Previous Behavior: WEM did not support a few BS counters.
New Behavior: WEM now supports BS counters.

Performance Indicator Changes

context Schema
- sfw-current-flows
- nat-current-flows
- nat44-current-flows
- nat64-current-flows
- bypass-nat-current-flows
- bypass-nat-ipv4-current-flows
- bypass-nat-ipv6-current-flows

dcca Schema
- ccr-inittimeout
- ccr-event
- cca-event
- cca-event-timeout

diameter-auth Schema
- aaa-req-received
- aaa-req-timeouts
- aaa-req-dropped

diameter Schema
- der-req-id-sent
- der-req-aka-chal-sent
- der-req-retried
- dea-chal-rcvd
- dea-acpt-rcvd
- dea-timeout
- dea-badauth
- dea-malformed
- dea-malformed-avp
- dea-dropped
- rar-req-rcvd
- raa-ans-acpt-sent
- aar-req-sent
- str-req-sent
- str-req-retried
- sta-ans-acpt-rcvd
- asr-req-rcvd
- asa-rsp-acpt-sent
- asa-rsp-rej-sent
- req-sock-write-err
- rsp-sock-write-err
- any-sock-read-err
- rem-disconnect
- loc-disconnect
- diameter-auth-msg-multiround
- diameter-auth-msg-success
- diameter-auth-msg-err-protocol
- diameter-auth-msg-err-transient
- diameter-auth-msg-err-permanent
- diameter-auth-msg-err-other
- aaa-req-received
- aaa-req-timeouts
- aaa-req-dropped

diameter

diameter-auth

diameter-auth-message

diameter-auth-message-multiround

diameter-auth-message-success

diameter-auth-message-err-protocol

diameter-auth-message-err-transient

diameter-auth-message-err-permanent

diameter-auth-message-err-other

aaa

aaa-request

aaa-request-received

aaa-request-timeouts

aaa-request-dropped
• ecs-first-http-request-url-redirections
• ecs-td-current-tethered-subscribers
• ecs-td-tethered-uplink-packets
• ecs-td-tethered-downlink-packets
• trm-rule-match-bypassed
• fp-eligible-flows
• fp-packets
• fp-failures
• video-readdress-req-redirected
• video-readdress-req-charging-action-hit
• video-readdress-resp-charging-action-hit
• video-readdress-skipped-pipelined-reqs
• video-readdress-load-balancer-failures
• video-readdress-flows-connected-to-video-server
• video-readdress-xhdr-insert-failed

egtpc Schema

• tun-sent-crebear-throttle-succeed
• tun-sent-crebear-throttle-queued
• tun-sent-crebear-throttle-dropped
• tun-sent-retranscrebear-throttle-succeed
• tun-sent-retranscrebear-throttle-queued
• tun-sent-retranscrebear-throttle-dropped
• tun-sent-updbearreq-throttle-succeed
• tun-sent-updbearreq-throttle-queued
• tun-sent-updbearreq-throttle-dropped
• tun-sent-retransupdbearreq-throttle-succeed
• tun-sent-retransupdbearreq-throttle-queued
• tun-sent-retransupdbearreq-throttle-dropped
• tun-sent-delbearreq-throttle-succeed
• tun-sent-delbearreq-throttle-queued
• tun-sent-delbearreq-throttle-dropped
• tun-sent-retransdelbearreq-throttle-succeed
• tun-sent-retransdelbearreq-throttle-queued
• tun-sent-retransdelbearreq-throttle-dropped
epdg Schema
- invalid-apn

gtpc Schema
- msgs-out-rate-limited
- msgs-out-rl-no-delay
- msgs-out-rl-queued
- msgs-out-rl-abort-queue
- msgs-out-rl-throttled
- msgs-inc-rate-limited
- msgs-inc-rl-scheduled
- msgs-inc-rl-curr-queued
- msgs-inc-rl-drop-queue
- msgs-inc-rl-throttled
- dyn-ipv4v6-attempt
- dyn-ipv4v6-success

hnbgw-access Schema
- s1ap-err-dupenb-ues1apid

hnbgw-rua Schema
- cs-connect-tx-est-cause-emergency
- cs-connect-tx-est-cause-normal
- ps-connect-tx-est-cause-emergency
- ps-connect-tx-est-cause-normal

icsr Schema
- switchover-number
- switchover-time
- switchover-reason
- audit_chassis_state
- audit_start_time
- audit_reason

imsa Schema
- dpca-msg-sgw-restore-rar-reject
• dpca-msg-sgw-restore-reval-timeout
• dpca-msg-sgw-restore-pending-updates
• dpca-imsa-tethering-flow-detected

**ipsg Schema**

• total-discard-msgs-partial-match-interim
• total_discard_msgs_partial_match_start

**lcs Schema**

• msg-lr-ans-timeout

**lma Schema**

• lma-txhbreqinitial
• lma-txhbreqretrans
• lma-txhbrsptotal
• lma-rxhbreqtotal
• lma-rxhbrsptotal
• lma-rxhbrsppbinderror
• lma-rxhbdecodeerror
• lma-rxhbinvalidbufflen
• lma-rxhbrspunknownpeer
• lma-rxhbrspseqnummismatch
• lma-rxhbrsprstctrmismatching
• lma-pathfailresttotal
• lma-pathfailrstctrmismatching
• lma-pathfailnohbrspcvd

**mag Schema**

• mag-txhbreqinitial
• mag-txhbreqretrans
• mag-txhbrsptotal
• mag-rxhbreqtotal
• mag-rxhbrsptotal
• mag-rxhbrsppbinderror
• mag-rxhbdecodeerror
- mag-rxhbdecodeerror
- mag-rxhbinvalidbufflen
- mag-rxhbrspunknownpeer
- mag-rxhbrspseqnummismatch
- mag-rxhbrsprstctrmissing
- mag-pathfailurestotal
- mag-pathfailrstctrchange
- mag-pathfailnohbrsprcvd

**p2p Schema**
- p2p-protocol-group
- p2p-duration-name
- p2p-uplnk-bytes-name
- p2p-dwlnk-bytes-name
- p2p-uplnk-pkts-name
- p2p-dwlnk-pkts-name

**pcc-policy Schema**
- total-gx-cca-sent
- total-gx-ccai-sent
- total-gx-ccau-sent
- total-gx-ccat-sent
- total-gx-rar-sess-release
- total-gx-raa-success-code
- total-gx-raa-failure-code
- total-gx-rar-ccr-collision
- total-gx-rar-transmitted

**saegw Schema**
- saegw-ipv4-colocated-pdn-dl-packets
- saegw-ipv4-colocated-pdn-dl-bytes
- saegw-ipv4-colocated-pdn-ul-packets
- saegw-ipv4-colocated-pdn-ul-bytes
- saegw-ipv6-colocated-pdn-dl-packets
- saegw-ipv6-colocated-pdn-dl-bytes
- saegw-ipv6-colocated-pdn-ul-packets
- saegw-ipv6-colocated-pdn-ul-bytes
- saegw-ipv4v6-colocated-pdn-ipv4-dl-packets
- saegw-ipv4v6-colocated-pdn-ipv4-dl-bytes
- saegw-ipv4v6-colocated-pdn-ipv4-ul-packets
- saegw-ipv4v6-colocated-pdn-ipv4-ul-bytes
- saegw-ipv4v6-colocated-pdn-ipv6-dl-packets
- saegw-ipv4v6-colocated-pdn-ipv6-dl-bytes
- saegw-ipv4v6-colocated-pdn-ipv6-ul-packets
- saegw-ipv4v6-colocated-pdn-ipv6-ul-bytes
- saegw-ipv4-sgw_anchored-pdn-dl-packets
- saegw-ipv4-sgw_anchored-pdn-dl-bytes
- saegw-ipv4-sgw_anchored-pdn-ipv4-dl-packets
- saegw-ipv4-sgw_anchored-pdn-ipv4-dl-bytes
- saegw-ipv4-sgw_anchored-pdn-ipv4-ul-packets
- saegw-ipv4-sgw_anchored-pdn-ipv4-ul-bytes
- saegw-ipv4-sgw_anchored-pdn-ipv6-dl-packets
- saegw-ipv4-sgw_anchored-pdn-ipv6-dl-bytes
- saegw-ipv6-sgw_anchored-pdn-dl-packets
- saegw-ipv6-sgw_anchored-pdn-dl-bytes
- saegw-ipv6-sgw_anchored-pdn-ul-packets
- saegw-ipv6-sgw_anchored-pdn-ul-bytes
- saegw-ipv6-sgw_anchored-pdn-ipv4-dl-packets
- saegw-ipv6-sgw_anchored-pdn-ipv4-dl-bytes
- saegw-ipv6-sgw_anchored-pdn-ipv4-ul-packets
- saegw-ipv6-sgw_anchored-pdn-ipv4-ul-bytes
- saegw-ipv6-sgw_anchored-pdn-ipv6-dl-packets
- saegw-ipv6-sgw_anchored-pdn-ipv6-dl-bytes
- saegw-ipv6-sgw_anchored-pdn-ipv6-ul-packets
- saegw-ipv6-sgw_anchored-pdn-ipv6-ul-bytes
- saegw-ipv4-pgw_anchored-pdn-dl-packets
- saegw-ipv4-pgw_anchored-pdn-dl-bytes
- saegw-ipv4-pgw_anchored-pdn-ipv4-dl-packets
- saegw-ipv4-pgw_anchored-pdn-ipv4-dl-bytes
- saegw-ipv4-pgw_anchored-pdn-ipv4-ul-packets
- saegw-ipv4-pgw_anchored-pdn-ipv4-ul-bytes
- saegw-ipv6-pgw_anchored-pdn-dl-packets
- saegw-ipv6-pgw_anchored-pdn-dl-bytes
- saegw-ipv6-pgw_anchored-pdn-ipv4-dl-packets
- saegw-ipv6-pgw_anchored-pdn-ipv4-dl-bytes
- saegw-ipv6-pgw_anchored-pdn-ipv6-dl-packets
- saegw-ipv6-pgw_anchored-pdn-ipv6-dl-bytes
- saegw-ipv6-pgw_anchored-pdn-ipv6-ul-packets
- saegw-ipv6-pgw_anchored-pdn-ipv6-ul-bytes
- saegw-ipv4v6-pgw_anchored-pdn-ipv4-dl-packets
- saegw-ipv4v6-pgw_anchored-pdn-ipv4-dl-bytes
- saegw-ipv4v6-pgw_anchored-pdn-ipv4-ul-packets
- saegw-ipv4v6-pgw_anchored-pdn-ipv4-ul-bytes
- saegw-ipv4v6-pgw_anchored-pdn-ipv6-dl-packets
- saegw-ipv4v6-pgw_anchored-pdn-ipv6-dl-bytes
- saegw-ipv4v6-pgw_anchored-pdn-ipv6-ul-packets
- saegw-ipv4v6-pgw_anchored-pdn-ipv6-ul-bytes
- saegw-ipv4-ggsn-pdn-dl-packets
- saegw-ipv4-ggsn-pdn-dl-bytes
- saegw-ipv4-ggsn-pdn-ul-packets
- saegw-ipv4-ggsn-pdn-ul-bytes
- saegw-ipv6-ggsn-pdn-dl-packets
- saegw-ipv6-ggsn-pdn-dl-bytes
- saegw-ipv6-ggsn-pdn-ul-packets
- saegw-ipv6-ggsn-pdn-ul-bytes
- saegw-ipv4v6-ggsn-pdn-ipv4-dl-packets
- saegw-ipv4v6-ggsn-pdn-ipv4-dl-bytes
- saegw-ipv4v6-ggsn-pdn-ipv4-ul-packets
- saegw-ipv4v6-ggsn-pdn-ipv4-ul-bytes
- saegw-ipv4v6-ggsn-pdn-ipv6-dl-packets
- saegw-ipv4v6-ggsn-pdn-ipv6-dl-bytes
- saegw-ipv4v6-ggsn-pdn-ipv6-ul-packets
- saegw-ipv4v6-ggsn-pdn-ipv6-ul-bytes
- saegw-ggsn-sessstat-bearact-emergency-def
- saegw-ggsn-sessstat-bearact-emergency-auth-imsi-def
- saegw-ggsn-sessstat-bearact-emergency-unauth-imsi-def
- saegw-ggsn-sessstat-bearact-emergency-only-imei-def
- saegw-ggsn-sessstat-bearact-ue-init-ded
- saegw-ggsn-sessstat-bearact-nw-init-ded
- saegw-ggsn-sessstat-bearact-emergency-ded
- saegw-ggsn-sessstat-bearact-emergency-auth-imsi-ded
- saegw-ggsn-sessstat-bearact-emergency-unauth-imsi-ded
- saegw-ggsn-sessstat-bearact-emergency-only-imei-ded
- saegw-ggsn-sessstat-bearact-nw-init-ded-att
• saegw-ggsn-sessstat-bearset-emergency-def
• saegw-ggsn-sessstat-bearset-emergency-auth-imsi-def
• saegw-ggsn-sessstat-bearset-emergency-unauth-imsi-def
• saegw-ggsn-sessstat-bearset-emergency-only-imei-def
• saegw-ggsn-sessstat-bearset-ue-init-ded
• saegw-ggsn-sessstat-bearset-nw-init-ded
• saegw-ggsn-sessstat-bearset-emergency-ded
• saegw-ggsn-sessstat-bearset-emergency-auth-imsi-ded
• saegw-ggsn-sessstat-bearset-emergency-unauth-imsi-ded
• saegw-ggsn-sessstat-bearset-emergency-only-imei-ded
• saegw-ggsn-sessstat-bearrel-nwdefadmin
• saegw-ggsn-sessstat-bearrel-nwdefgtp
• saegw-ggsn-sessstat-bearrel-nwdefsgw
• saegw-ggsn-sessstat-bearrel-nwdefsgsn
• saegw-ggsn-sessstat-bearrel-nwdefmme
• saegw-ggsn-sessstat-bearrel-nwdeadmin
• saegw-ggsn-sessstat-bearrel-nwdedgtp
• saegw-ggsn-sessstat-bearrel-nwdedmme
• saegw-ggsn-sessstat-bearrel-nwdeddefbear
• saegw-ggsn-sessstat-bearrel-nwdedgxdisc
• saegw-ggsn-sessstat-bearrelfail-def
• saegw-ggsn-sessstat-bearrelfail-ded
• saegw-ggsn-sessstat-bearrej-def
• saegw-ggsn-sessstat-bearrej-ded
• saegw-ggsn-sessstat-bearrej-emergency-def
• saegw-ggsn-sessstat-bearrej-emergency-ded
• saegw-ggsn-sessstat-bearrej-nores
• saegw-ggsn-sessstat-bearrej-uereq
• saegw-ggsn-sessstat-bearrej-uereq-nores
• saegw-ggsn-sessstat-bearrej-misapn
• saegw-ggsn-sessstat-bearrej-nwreq
• saegw-ggsn-sessstat-bearrej-nwreq-nores
• saegw-ggsn-sessstat-bearrej-nwreq-nomem
• saegw-ggsn-sessstat-bearrej-nwreq-sysfail
• saegw-ggsn-sessstat-bearrej-apnmode
• saegw-ggsn-sessstat-bearrej-pdn
• saegw-ggsn-sessstat-bearrej-apnrestr
• saegw-ggsn-sessstat-bearrej-subsauth
• saegw-ggsn-sessstat-bearrej-subsaddrnotallow
• saegw-ggsn-sessstat-bearrej-subsaddrnotalloc
• saegw-ggsn-sessstat-bearrej-dynaddrnotalloc
• saegw-ggsn-sessstat-bearrej-subsaddnotpres
• saegw-ggsn-sessstat-bearrej-subsaddrnotalloc
• saegw-ggsn-sessstat-bearrej-subsaddrnotpres
• saegw-ggsn-sessstat-bearmod-ueinit
• saegw-ggsn-sessstat-bearmod-nwinit
• saegw-ggsn-sessstat-bearmod-ueqos
• saegw-ggsn-sessstat-bearmod-uetft
• saegw-ggsn-sessstat-bearmod-nwqos
• saegw-ggsn-sessstat-bearmod-nwtft
• saegw-ggsn-sessstat-bearmodfail-ueinit
• saegw-ggsn-sessstat-bearmodfail-nwinit
• saegw-ggsn-sessstat-bearmodfail-uenores
• saegw-ggsn-sessstat-bearmodfail-uesemtft
• saegw-ggsn-sessstat-bearmodfail-uesynftft
• saegw-ggsn-sessstat-bearmodfail-uesempkt
• saegw-ggsn-sessstat-bearmodfail-uesynpkt
• saegw-ggsn-sessstat-bearmodfail-nwnores
• saegw-ggsn-sessstat-bearmodfail-nwnomem
• saegw-ggsn-sessstat-bearmodfail-nwsysfail
• saegw-ggsn-sessstat-bearmodfail-nwsemftf
• saegw-ggsn-sessstat-bearmodfail-nwsynftft
• saegw-ggsn-sessstat-bearmodfail-nwsempkt
• saegw-ggsn-sessstat-bearmodfail-nwsynpkt
• saegw-ggsn-sessstat-bearmodfail-qos-uenores
• saegw-ggsn-sessstat-bearmodfail-qos-uesemtft
• saegw-ggsn-sessstat-bearmodfail-qos-uesynftft
• saegw-ggsn-sessstat-bearmodfail-qos-uesempkt
• saegw-ggsn-sessstat-bearmodfail-qos-uesynpkt
• saegw-ggsn-sessstat-bearmodfail-qos-nwnores
- `saegw-ggsn-sessstat-bearmodfail-qos-nwnomem`
- `saegw-ggsn-sessstat-bearmodfail-qos-nwsysfail`
- `saegw-ggsn-sessstat-bearmodfail-qos-nwsemtif`
- `saegw-ggsn-sessstat-bearmodfail-qos-nwsyntft`
- `saegw-ggsn-sessstat-bearmodfail-qos-nwempkt`
- `saegw-ggsn-sessstat-bearmodfail-qos-nwsysfail`
- `saegw-ggsn-sessstat-bearmodfail-qos-nwsemtft`
- `saegw-ggsn-sessstat-bearmodfail-qos-nwsyntft`
- `saegw-ggsn-sessstat-bearmodfail-qos-nwempkt`
- `saegw-ggsn-sessstat-bearmodfail-qos-nwsysfail`
- `saegw-ggsn-sessstat-bearmodfail-qos-nwsemtft`
- `saegw-ggsn-sessstat-bearmodfail-qos-nwsyntft`
- `saegw-ggsn-sessstat-beardel-ded`
- `saegw-ggsn-sessstat-nw-init-qos-update-att`
- `saegw-ggsn-sessstat-nw-init-no-qos-update-att`
- `saegw-ggsn-sessstat-nw-init-bearer-fail-cause`
- `saegw-ggsn-sessstat-ipv4addaloc`
- `saegw-ggsn-sessstat-ipaddaloc-ipv4loacalpool`
- `saegw-ggsn-sessstat-ipaddaloc-ipv4staticaddr`
- `saegw-ggsn-sessstat-ipaddaloc-ipv4radaddr`
- `saegw-ggsn-sessstat-ipaddaloc-ipv6addaloc`
- `saegw-ggsn-sessstat-ipaddaloc-ipv6auto`
- `saegw-ggsn-subplmnstat-homesubact`
- `saegw-ggsn-subplmnstat-homesubsetup`
- `saegw-ggsn-subplmnstat-homesubrel`
- `saegw-ggsn-subplmnstat-roamsubact`
- `saegw-ggsn-subplmnstat-roamsubsetup`
- `saegw-ggsn-subplmnstat-roamsubrel`
- `saegw-ggsn-subplmnstat-visitsubact`
- `saegw-ggsn-subplmnstat-visitsubsetup`
- `saegw-ggsn-subplmnstat-visitsubrel`
- `saegw-ggsn-handoverstat-intersgsnatt`
- `saegw-ggsn-handoverstat-intersgsnsucc`
- `saegw-ggsn-handoverstat-intersgsnfail`
- `saegw-ggsn-handoverstat-gnptolteatt`
- `saegw-ggsn-handoverstat-gnptoltesucc`
- `saegw-ggsn-handoverstat-gnptoltefail`
- `saegw-ggsn-handoverstat-ltetogngpatt`
- `saegw-ggsn-handoverstat-ltetogngpsucc`
- `saegw-ggsn-handoverstat-ltetogngpfail`
- saegw-ggsn-subqosstat-bearact-qci1
- saegw-ggsn-subqosstat-bearact-qci2
- saegw-ggsn-subqosstat-bearact-qci3
- saegw-ggsn-subqosstat-bearact-qci4
- saegw-ggsn-subqosstat-bearact-qci5
- saegw-ggsn-subqosstat-bearact-qci6
- saegw-ggsn-subqosstat-bearact-qci7
- saegw-ggsn-subqosstat-bearact-qci8
- saegw-ggsn-subqosstat-bearact-qci9
- saegw-ggsn-subqosstat-bearact-qcinongbr
- saegw-ggsn-subqosstat-bearact-qcigbr
- saegw-ggsn-subqosstat-bearset-qci1
- saegw-ggsn-subqosstat-bearset-qci2
- saegw-ggsn-subqosstat-bearset-qci3
- saegw-ggsn-subqosstat-bearset-qci4
- saegw-ggsn-subqosstat-bearset-qci5
- saegw-ggsn-subqosstat-bearset-qci6
- saegw-ggsn-subqosstat-bearset-qci7
- saegw-ggsn-subqosstat-bearset-qci8
- saegw-ggsn-subqosstat-bearset-qci9
- saegw-ggsn-subqosstat-bearset-qcinongbr
- saegw-ggsn-subqosstat-bearset-qcigbr
- saegw-ggsn-subqosstat-bearrel-qci1
- saegw-ggsn-subqosstat-bearrel-qci2
- saegw-ggsn-subqosstat-bearrel-qci3
- saegw-ggsn-subqosstat-bearrel-qci4
- saegw-ggsn-subqosstat-bearrel-qci5
- saegw-ggsn-subqosstat-bearrel-qci6
- saegw-ggsn-subqosstat-bearrel-qci7
- saegw-ggsn-subqosstat-bearrel-qci8
- saegw-ggsn-subqosstat-bearrel-qci9
- saegw-ggsn-subqosstat-bearrel-qcinongbr
- saegw-ggsn-subqosstat-bearrel-qcigbr
- saegw-ggsn-subdatastat-totulpktfwd
- saegw-ggsn-subdatastat-ulpktfwd-qci1
- saegw-ggsn-subdatastat-ulpktfwd-qci2
- saegw-ggsn-subdatastat-ulpktfwd-qci3
- saegw-ggsn-subdatastat-ulpktfwd-qci4
- saegw-ggsn-subdatastat-ulpktfwd-qci5
- saegw-ggsn-subdatastat-ulpktfwd-qci6
- saegw-ggsn-subdatastat-ulpktfwd-qci7
- saegw-ggsn-subdatastat-ulpktfwd-qci8
- saegw-ggsn-subdatastat-ulpktfwd-qci9
- saegw-ggsn-subdatastat-ulpktfwd-stdqcinongbr
- saegw-ggsn-subdatastat-ulpktfwd-stdqcigbr
- saegw-ggsn-subdatastat-ulpktfwd-qcinongbr
- saegw-ggsn-subdatastat-ulpktfwd-qcigbr
- saegw-ggsn-subdatastat-ulpktfwd-totgbr
- saegw-ggsn-subdatastat-ulpktfwd-totnongbr
- saegw-ggsn-subdatastat-totulbytefwd
- saegw-ggsn-subdatastat-ulbytefwd-qci1
- saegw-ggsn-subdatastat-ulbytefwd-qci2
- saegw-ggsn-subdatastat-ulbytefwd-qci3
- saegw-ggsn-subdatastat-ulbytefwd-qci4
- saegw-ggsn-subdatastat-ulbytefwd-qci5
- saegw-ggsn-subdatastat-ulbytefwd-qci6
- saegw-ggsn-subdatastat-ulbytefwd-qci7
- saegw-ggsn-subdatastat-ulbytefwd-qci8
- saegw-ggsn-subdatastat-ulbytefwd-qci9
- saegw-ggsn-subdatastat-ulbytefwd-stdqcinongbr
- saegw-ggsn-subdatastat-ulbytefwd-stdqcigbr
- saegw-ggsn-subdatastat-ulbytefwd-qcinongbr
- saegw-ggsn-subdatastat-ulbytefwd-qcigbr
- saegw-ggsn-subdatastat-ulbytefwd-totgbr
- saegw-ggsn-subdatastat-ulbytefwd-totnongbr
- saegw-ggsn-subdatastat-totdlpktfwd
- saegw-ggsn-subdatastat-dlpktfwd-qci1
- saegw-ggsn-subdatastat-dlpktfwd-qci2
• saegw-ggsn-subdatastat-dlpktfwd-qci3
• saegw-ggsn-subdatastat-dlpktfwd-qci4
• saegw-ggsn-subdatastat-dlpktfwd-qci5
• saegw-ggsn-subdatastat-dlpktfwd-qci6
• saegw-ggsn-subdatastat-dlpktfwd-qci7
• saegw-ggsn-subdatastat-dlpktfwd-qci8
• saegw-ggsn-subdatastat-dlpktfwd-qci9
• saegw-ggsn-subdatastat-dlpktfwd-stdqcinongbr
• saegw-ggsn-subdatastat-dlpktfwd-stdqcigbr
• saegw-ggsn-subdatastat-dlpktfwd-qcinongbr
• saegw-ggsn-subdatastat-dlpktfwd-qcigbr
• saegw-ggsn-subdatastat-dlpktfwd-totgbr
• saegw-ggsn-subdatastat-dlpktfwd-totnongbr
• saegw-ggsn-subdatastat-totdlbytefwd
• saegw-ggsn-subdatastat-dlbytefwd-qci1
• saegw-ggsn-subdatastat-dlbytefwd-qci2
• saegw-ggsn-subdatastat-dlbytefwd-qci3
• saegw-ggsn-subdatastat-dlbytefwd-qci4
• saegw-ggsn-subdatastat-dlbytefwd-qci5
• saegw-ggsn-subdatastat-dlbytefwd-qci6
• saegw-ggsn-subdatastat-dlbytefwd-qci7
• saegw-ggsn-subdatastat-dlbytefwd-qci8
• saegw-ggsn-subdatastat-dlbytefwd-qci9
• saegw-ggsn-subdatastat-dlbytefwd-stdqcinongbr
• saegw-ggsn-subdatastat-dlbytefwd-stdqcigbr
• saegw-ggsn-subdatastat-dlbytefwd-qcinongbr
• saegw-ggsn-subdatastat-dlbytefwd-qcigbr
• saegw-ggsn-subdatastat-dlbytefwd-totgbr
• saegw-ggsn-subdatastat-dlbytefwd-totnongbr
• saegw-ggsn-subdatastat-totulpktdrop
• saegw-ggsn-subdatastat-ulpktdrop-qci1
• saegw-ggsn-subdatastat-ulpktdrop-qci2
• saegw-ggsn-subdatastat-ulpktdrop-qci3
• saegw-ggsn-subdatastat-ulpktdrop-qci4
- saegw-ggsn-subdatastat-ulpktdrop-qci5
- saegw-ggsn-subdatastat-ulpktdrop-qci6
- saegw-ggsn-subdatastat-ulpktdrop-qci7
- saegw-ggsn-subdatastat-ulpktdrop-qci8
- saegw-ggsn-subdatastat-ulpktdrop-qci9
- saegw-ggsn-subdatastat-ulpktdrop-stdqcinongbr
- saegw-ggsn-subdatastat-ulpktdrop-stdqcigbr
- saegw-ggsn-subdatastat-ulpktdrop-qcinongbr
- saegw-ggsn-subdatastat-ulpktdrop-qcigbr
- saegw-ggsn-subdatastat-ulpktdrop-totgbr
- saegw-ggsn-subdatastat-ulpktdrop-totnongbr
- saegw-ggsn-subdatastat-totulbytedrop
- saegw-ggsn-subdatastat-ulbytedrop-qci1
- saegw-ggsn-subdatastat-ulbytedrop-qci2
- saegw-ggsn-subdatastat-ulbytedrop-qci3
- saegw-ggsn-subdatastat-ulbytedrop-qci4
- saegw-ggsn-subdatastat-ulbytedrop-qci5
- saegw-ggsn-subdatastat-ulbytedrop-qci6
- saegw-ggsn-subdatastat-ulbytedrop-qci7
- saegw-ggsn-subdatastat-ulbytedrop-qci8
- saegw-ggsn-subdatastat-ulbytedrop-qci9
- saegw-ggsn-subdatastat-ulbytedrop-stdqcinongbr
- saegw-ggsn-subdatastat-ulbytedrop-stdqcigbr
- saegw-ggsn-subdatastat-ulbytedrop-qcinongbr
- saegw-ggsn-subdatastat-ulbytedrop-qcigbr
- saegw-ggsn-subdatastat-ulbytedrop-totgbr
- saegw-ggsn-subdatastat-ulbytedrop-totnongbr
- saegw-ggsn-subdatastat-totdlpktdrop
- saegw-ggsn-subdatastat-dlpktdrop-qci1
- saegw-ggsn-subdatastat-dlpktdrop-qci2
- saegw-ggsn-subdatastat-dlpktdrop-qci3
- saegw-ggsn-subdatastat-dlpktdrop-qci4
- saegw-ggsn-subdatastat-dlpktdrop-qci5
- saegw-ggsn-subdatastat-dlpktdrop-qci6
• saegw-ggsn-subdatastat-dlpktdrop-qci7
• saegw-ggsn-subdatastat-dlpktdrop-qci8
• saegw-ggsn-subdatastat-dlpktdrop-qci9
• saegw-ggsn-subdatastat-dlpktdrop-stdqcinongbr
• saegw-ggsn-subdatastat-dlpktdrop-stdqcigbr
• saegw-ggsn-subdatastat-dlpktdrop-qcinongbr
• saegw-ggsn-subdatastat-dlpktdrop-qcigbr
• saegw-ggsn-subdatastat-dlpktdrop-totgbr
• saegw-ggsn-subdatastat-dlpktdrop-totnongbr
• saegw-ggsn-subdatastat-totdlbytedrop
• saegw-ggsn-subdatastat-dlbytedrop-qci1
• saegw-ggsn-subdatastat-dlbytedrop-qci2
• saegw-ggsn-subdatastat-dlbytedrop-qci3
• saegw-ggsn-subdatastat-dlbytedrop-qci4
• saegw-ggsn-subdatastat-dlbytedrop-qci5
• saegw-ggsn-subdatastat-dlbytedrop-qci6
• saegw-ggsn-subdatastat-dlbytedrop-qci7
• saegw-ggsn-subdatastat-dlbytedrop-qci8
• saegw-ggsn-subdatastat-dlbytedrop-qci9
• saegw-ggsn-subdatastat-dlbytedrop-stdqcinongbr
• saegw-ggsn-subdatastat-dlbytedrop-stdqcigbr
• saegw-ggsn-subdatastat-dlbytedrop-qcinongbr
• saegw-ggsn-subdatastat-dlbytedrop-qcigbr
• saegw-ggsn-subdatastat-dlbytedrop-totgbr
• saegw-ggsn-subdatastat-dlbytedrop-totnongbr
• saegw-ggsn-subdatastat-totulpktdropmbrexc
• saegw-ggsn-subdatastat-ulpktdropmbrexc-qci1
• saegw-ggsn-subdatastat-ulpktdropmbrexc-qci2
• saegw-ggsn-subdatastat-ulpktdropmbrexc-qci3
• saegw-ggsn-subdatastat-ulpktdropmbrexc-qci4
• saegw-ggsn-subdatastat-ulpktdropmbrexc-qci5
• saegw-ggsn-subdatastat-ulpktdropmbrexc-qci6
• saegw-ggsn-subdatastat-ulpktdropmbrexc-qci7
• saegw-ggsn-subdatastat-ulpktdropmbrexc-qci8
- saegw-ggsn-subdatastat-ulpktdropmbrexc-qci9
- saegw-ggsn-subdatastat-ulpktdropmbrexc-stdqcinongbr
- saegw-ggsn-subdatastat-ulpktdropmbrexc-stdqcigbr
- saegw-ggsn-subdatastat-ulpktdropmbrexc-qcinongbr
- saegw-ggsn-subdatastat-ulpktdropmbrexc-qcigbr
- saegw-ggsn-subdatastat-ulpktdropmbrexc-totgbr
- saegw-ggsn-subdatastat-ulpktdropmbrexc-totnongbr
- saegw-ggsn-subdatastat-totulbytedropmbrexc
- saegw-ggsn-subdatastat-ulbytedropmbrexc-qci1
- saegw-ggsn-subdatastat-ulbytedropmbrexc-qci2
- saegw-ggsn-subdatastat-ulbytedropmbrexc-qci3
- saegw-ggsn-subdatastat-ulbytedropmbrexc-qci4
- saegw-ggsn-subdatastat-ulbytedropmbrexc-qci5
- saegw-ggsn-subdatastat-ulbytedropmbrexc-qci6
- saegw-ggsn-subdatastat-ulbytedropmbrexc-qci7
- saegw-ggsn-subdatastat-ulbytedropmbrexc-qci8
- saegw-ggsn-subdatastat-ulbytedropmbrexc-qci9
- saegw-ggsn-subdatastat-ulbytedropmbrexc-stdqcinongbr
- saegw-ggsn-subdatastat-ulbytedropmbrexc-stdqcigbr
- saegw-ggsn-subdatastat-ulbytedropmbrexc-qcinongbr
- saegw-ggsn-subdatastat-ulbytedropmbrexc-qcigbr
- saegw-ggsn-subdatastat-ulbytedropmbrexc-totgbr
- saegw-ggsn-subdatastat-ulbytedropmbrexc-totnongbr
- saegw-ggsn-subdatastat-totdlpktdropmbrexc
- saegw-ggsn-subdatastat-dlpktdropmbrexc-qci1
- saegw-ggsn-subdatastat-dlpktdropmbrexc-qci2
- saegw-ggsn-subdatastat-dlpktdropmbrexc-qci3
- saegw-ggsn-subdatastat-dlpktdropmbrexc-qci4
- saegw-ggsn-subdatastat-dlpktdropmbrexc-qci5
- saegw-ggsn-subdatastat-dlpktdropmbrexc-qci6
- saegw-ggsn-subdatastat-dlpktdropmbrexc-qci7
- saegw-ggsn-subdatastat-dlpktdropmbrexc-qci8
- saegw-ggsn-subdatastat-dlpktdropmbrexc-qci9
- saegw-ggsn-subdatastat-dlpktdropmbrexc-stdqcinongbr
Web Element Manager Changes in Release 15.0

WEM Enhancements for Jan 31, 2014

- saegw-ggsn-subdatastat-dlpktdropmbrexc-stdqcigbr
- saegw-ggsn-subdatastat-dlpktdropmbrexc-qcinongbr
- saegw-ggsn-subdatastat-dlpktdropmbrexc-qcigbr
- saegw-ggsn-subdatastat-dlpktdropmbrexc-totgbr
- saegw-ggsn-subdatastat-dlpktdropmbrexc-totnongbr
- saegw-ggsn-subdatastat-totdlbytedropmbrexc
- saegw-ggsn-subdatastat-dlbytedropmbrexc-qci1
- saegw-ggsn-subdatastat-dlbytedropmbrexc-qci2
- saegw-ggsn-subdatastat-dlbytedropmbrexc-qci3
- saegw-ggsn-subdatastat-dlbytedropmbrexc-qci4
- saegw-ggsn-subdatastat-dlbytedropmbrexc-qci5
- saegw-ggsn-subdatastat-dlbytedropmbrexc-qci6
- saegw-ggsn-subdatastat-dlbytedropmbrexc-qci7
- saegw-ggsn-subdatastat-dlbytedropmbrexc-qci8
- saegw-ggsn-subdatastat-dlbytedropmbrexc-qci9
- saegw-ggsn-subdatastat-dlbytedropmbrexc-stdqcinongbr
- saegw-ggsn-subdatastat-dlbytedropmbrexc-stdqcigbr
- saegw-ggsn-subdatastat-dlbytedropmbrexc-qcinongbr
- saegw-ggsn-subdatastat-dlbytedropmbrexc-qcigbr
- saegw-ggsn-subdatastat-dlbytedropmbrexc-totgbr
- saegw-ggsn-subdatastat-dlbytedropmbrexc-totnongbr
- saegw-ggsn-apnambratelimit-ulpktdrop
- saegw-ggsn-apnambratelimit-dlpktdrop
- saegw-ggsn-apnambratelimit-ulbytedrop
- saegw-ggsn-apnambratelimit-dlbytedrop

samog Schema

- mrme-total-dropped
- mrme-total-rad-send-failure
- mrme-total-discard-start-partial-match
- mrme-total-discard-interim-partial-match
- mrme-total_discard_congestion_policy_applied
- mrme-total_discard_invalid_length
- mrme-total_discard_invalid_eap
- mrme-disconnect-nas
- mrme-dhcp-msg-dropped
- mrme-dhcp-discard-exceeded-max-size
- mrme-dhcp-discard-non-existing-session
- mrme-dhcp-discard-giaddr-mismatch
- mrme-dhcp-discard-hw-type-len-unsupported
- mrme-reauthor-rar-attempt
- mrme-reauthor-rar-failure
- mrme-reauthor-rar-success
- mrme-eap-rxmobile-eap-initial-req
- mrme-eap-rxmobile-non-identity-start
- mrme-eap-rxmobile-eap-disc-code
- mrme-eap-rxmobile-invalid-imsi
- mrme-eap-rxmobile-invalid-nai
- mrme-eap-rxmobile-eap-failure-rcvd
- mrme-eap-rxmobile-eap-msgs-from-server-discarded
- mrme-eap-rxmobile-eap-total-dropped
- mrme-eap-rxmobile-eap-drop-code

sgsn Schema

- 2G-network-sharing-supp-ue
- 2G-network-sharing-non-supp-ue
- 3G-sec-actv-rej-coll-with-net-init-req
- 2G-sec-actv-rej-coll-with-net-init-req

sgs-vlr Schema

- localupd-timeout-tx
- localupd-timeout-retx
- localupd-timeout-rx

NAT Realm Schema

- nat-rlm-bytes-tx
- nat-rlm-flows
Feature Changes

PCFUnreachable Alarm Was Not Getting Cleared Automatically

A correlation rule has been added to the PCFUnreachable trap. The PCFUnreachable alarm gets cleared when the PCFReachable alarm is received.

**Previous Behavior:** The PCFUnreachable alarm was not getting automatically cleared when the PCFReachable alarm was generated.

**New Behavior:** The PCFUnreachable alarm gets cleared when the PCFReachable alarm is received.
WEM Enhancements for September 30, 2013

WEM Feature Changes as of September 30, 2013

This section provides information on WEM feature changes in release 15.0.

Important: For more information regarding features in this section, refer to the Web Element Manager Installation and Administration Guide for this release.

New WEM Features

This section identifies new WEM features available in release 15.0.

WEM 12.0.2207 - GUI Cannot be accessed using Java 1.7

From this release, WEM GUI supports JRE 1.6 and 1.7. JRE version 1.5 and below are restricted.

WEM: Link to diagnostic of a card needed in the NE front view

In NE Front/Rear view, a link to Card Diagnostics screen has been added in the menu. This link is invoked when you right click on the link.

[WEM_RM_007] ASCII PM Files selectable for bulkstats reduction

WEM provides screen available from the WEM > Accounting >Bulkstat XML/ASCII file configuration path for you to select a list of counters that you intend to report in the XML/ASCII files.

Bulk statistics presentation change

This release onward, there has been presentation change in the way bulk statistics are displayed on WEM. The display string for all the counters has been replaced by counter names in that schema.xml file. Categories are available only for SGSN, SS7RD, SS7LINK, and PS_GW_SCCP; all other schemas have no categories available.

15.0 onwards, only Linux builds will be released

This release onward, WEM builds would be released for Linux platforms only. WEM on Solaris platforms will not be released. If you are using older version of WEM running on Solaris platform, you will need to migrate to Linux platforms.

Regarding Pool Group stats in the WEM reporting

WEM now supports pool group name based reports.

Modified WEM Features

This section identifies WEM features modified in release 15.0.
WEM 14.0 SNMP not displaying some new traps

WEM now syncs and supports all the alarms available on ASR5k.

**Previous Behavior:** All the alarms on ASR5k were not visible from WEM.

**New Behavior:** All the alarms on ASR5k are synced and supported on WEM

MT sgs-vlr schema is not supported by WEM, but exists in ASR5k

WEM now supports SGs statistics per VLR and is accessible through WEM GUI. XML/ASCII file generation is also supported for sgs_vlr schema.

**Previous Behavior:** SGs statistics per VLR was not accessible through WEM GUI.

**New Behavior:** SGs statistics per VLR is now accessible through WEM GUI. XML/ASCII file generation is also supported for sgs_vlr schema.

**[WEM_RM_003]** Sync up for all bulk stats counters available on the ASR5K

WEM now syncs and supports all counters on ASR5k.

**Previous Behavior:** All counters on ASR5k were not visible through WEM GUI.

**New Behavior:** WEM now syncs and supports all the counters on ASR5k.

**[WEM_RM_003]** Sync up for pre 15.0 bulk stats counters on the ASR5K

WEM now syncs up with ASR5k and supports all the bulk stats available on ASR5k prior to 15.0 releases.

**Previous Behavior:** All bulk stats supported on ASR5k prior to release 15.0 were not visible through WEM GUI.

**New Behavior:** WEM now syncs and supports all the bulk stats available on ASR5k, prior to release 15.0.

**[WEM_RM_003]** Sync up for pre 15.0 alarms available on the ASR5K

WEM now syncs up with ASR5k and supports all the alarms available on ASR5k prior to 15.0 releases.

**Previous Behavior:** All alarms supported on ASR5k prior to release 15.0 were not visible through WEM GUI.

**New Behavior:** WEM now syncs and supports all the alarms available on ASR5k, prior to release 15.0.

CounterDataType mismatch between ASR5K and EMS

WEM now syncs up with ASR5k and matches with the CounterDataType on ASR5k.

**Previous Behavior:** All CounterDataType supported on ASR5k prior to release 15.0 were not visible through WEM GUI.

**New Behavior:** WEM now syncs and supports all the CounterDataType available on ASR5k, prior to release 15.0.

WEM Fault Management Changes as of September 30, 2013

This section provides information on WEM fault management changes in release 15.0.

None for this release.
WEM Configuration Management Changes as of September 30, 2013

This section provides information on WEM configuration management changes in release 15.0.
None for this release.

WEM Accounting Management Changes as of September 30, 2013

This section provides information on WEM accounting management changes in release 15.0.
None for this release.

WEM Performance Management Changes as of September 30, 2013

This section provides information on WEM performance management changes in release 15.0.
None for this release.