Cisco ASR 5000 Series Release Change Reference

Release 11.0 to Releases 12.0, 12.1, and 12.2

Last Updated April 30, 2013

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

Text Part Number: OL-25191-20

Cisco ASR 5000 Series Release Change Reference

TABLE OF CONTENTS

Chapter 2:
Fault Management

Chapter 3: Configuration Management

Chapter 4: Accounting Management

Chapter 5: Performance Management

Chapter 6: Security Management

ABOUT THIS GUIDE

This document pertains to features and functionality that run on and/or that are related to the Cisco® ASR 5000 Chassis, formerly the Starent Networks ST40.

Conventions Used

The following tables describe the conventions used throughout this documentation.

Icon	Notice Type	Description
	Information Note	Provides information about important features or instructions.
	Caution	Alerts you of potential damage to a program, device, or system.
	Warning	Alerts you of potential personal injury or fatality. May also alert you of potential electrical hazards.
	Electro-Static Discharge (ESD)	Alerts you to take proper grounding precautions before handling a product.

Typeface Conventions	Description
`Text represented as a screen display`	This typeface represents displays that appear on your terminal screen, for example: `Login:`
Text represented as **`commands`**	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.
Text represented as a **`command`** *`variable`*	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.
Text represented as menu or sub-menu names	This typeface represents menus and sub-menus that you access within a software application, for example: Click the File menu, then click New

Command Syntax Conventions	Description
{ **`keyword`** or *`variable`* }	Required keywords and variables are surrounded by grouped brackets. Required keywords and variables are those components that are required to be entered as part of the command syntax.
[**`keyword`** or *`variable`*]	Optional keywords or variables, or those that a user may or may not choose to use, are surrounded by square brackets.

Command Syntax Conventions	Description
|	With some commands there may be a group of variables from which the user chooses one. These are called alternative variables and are documented by separating each variable with a vertical bar (also known as a pipe filter). Pipe filters can be used in conjunction with required or optional keywords or variables. For example: **{ nonce | timestamp }** OR [**count** *number_of_packets* |**size** *number_of_bytes*]

Contacting Customer Support

Use the information in this section to contact customer support.

For New Customers: 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 is required to this site. Please contact your local sales or service representative for additional information.

For Existing Customers with support contracts through Starent Networks: Refer to the support area of https://support.starentnetworks.com/ for up-to-date product documentation or to submit a service request. A valid username and password is required to this site. Please contact your local sales or service representative for additional information.

IMPORTANT

For warranty and repair information, please be sure to include the Return Material Authorization (RMA) tracking number on the outside of the package.

CHAPTER 1
NEW FEATURE SUMMARY

This chapter identifies features and functionality added to or modified in Releases 12.0, 12.1, and 12.2.

Topics covered in this chapter are:

Related Documents

Additional information on the items listed in this chapter is available in the documentation listed in the table below.

Table 1-1 Released Documentation

Document
Cisco ASR 5000 Series Product Overview Guide
Cisco ASR 5000 Series Packet Data Serving Node Administration Guide
Cisco ASR 5000 Series SNMP MIB Reference
Cisco ASR 5000 Series Gateway GPRS Support Node Administration Guide
Cisco Web Element Manager Installation and Administration Guide
Cisco ASR 5000 Command Line Interface Reference
Cisco ASR 5000 Series Enhanced Charging Services Administration Guide
Cisco ASR 5000 Series Access Service Network Gateway Administration Guide
Cisco ASR 5000 Series AAA and GTP Interface Administration and Reference
Cisco ASR 5000 Series Release 11.0 to Release 12.x Change Reference
Cisco ASR 5000 Series Application Detection and Control Administration Guide
Cisco ASR 5000 Series IP Services Gateway Administration Guide
Cisco ASR 5000 Series Packet Data Interworking Function Administration Guide
Cisco ASR 5000 Series Personal Stateful Firewall Administration Guide
Cisco ASR 5000 Series Thresholding Configuration Guide
Cisco ASR 5000 Series Serving GPRS Support Node Administration Guide
Cisco ASR 5000 System Administration Guide
Cisco ASR 5000 Series Home Agent Administration Guide
Cisco ASR 5000 Series InTracer Installation and Administration Guide
Cisco ASR 5000 Series HRPD Serving Gateway Administration Guide
Cisco ASR 5000 Series Packet Data Network Gateway Administration Guide
Cisco ASR 5000 Series Serving Gateway Administration Guide
Cisco ASR 5000 Series Mobility Management Entity Administration Guide
Cisco ASR 5000 Series Lawful Intercept Configuration Guide
Cisco ASR 5000 Series Statistics and Counters Reference
Cisco ASR 5000 Series Network Address Translation Administration Guide
Cisco ASR 5000 Series Mobility Unified Reporting System Installation and Administration Guide
Cisco ASR 5000 Installation Guide
Cisco ASR 5000 Series Femto Network Gateway Administration Guide

Table 1-1 Released Documentation (continued)

Document
Cisco ASR 5000 Series 3G Home NodeB Gateway Administration Guide
Cisco ASR 5000 Traffic Performance Optimization Administration Guide
Cisco ASR 5000 Mobile Services Edge Gateway - 3G Administration Guide
Cisco ASR 5000 Series Mobile Video Gateway Administration Guide
Cisco ASR 5000 Series Intelligent Policy Control Function Administration Guide
Cisco ASR 5000 Series Subscriber Service Controller Installation and Configuration Guide
Cisco ASR 5000 Series Policy Provisioning Tool Installation and Configuration Guide
Cisco ASR 5000 Series LTE Doc Set
Cisco ASR 5000 Series PDSN Doc Set
Cisco ASR 5000 Series UMTS Doc Set
Open Source Software Licenses for Cisco ASR 5000 Series Multimedia Network Core Platform
Open Source Software Licenses for Cisco GTPP Storage Server
Open Source Software Licenses for Cisco Mobility Unified Reporting System
Open Source Software Licenses for Cisco Local External Storage Server
Open Source Software Licenses for Cisco Policy Provisioning Tool
Open Source Software Licenses for Cisco Subscriber Service Controller
Open Source Software Licenses for Cisco Web Element Manager
Open Source Software Licenses for Cisco InTracer

The latest versions of the documentation are available on Cisco.com:

http://www.cisco.com/en/US/products/ps11072/tsd_products_support_series_home.html

Common Features in Release 12.0

This section provides information on new features that are common to products in Release 12.0.

Bearer-Usage AVP Value for Primary/Secondary Contexts - Behavioral Change

This Diameter-related behavioral change is applicable to all products that use the Gy interface.

In the earlier releases, the Bearer-Usage AVP was encoded with the value GENERAL(0) irrespective of whether the context is primary or secondary in the Diameter Gy CCR message.

In the current release, the Bearer-Usage AVP will be encoded with the value GENERAL(0) for Primary-PDP context/default bearer and with the value DEDICATED(2) for all secondary-PDPs/dedicated bearers.

Call Termination for CCA-I with Error-result Code - Behavioral Change

This Diameter-related behavioral change is applicable to all products that use the Gx interface.

In the earlier releases, when there were no static rules configured in the chassis and if the PCRF returns a error-result code in CCA-I with CCFH action as continue, then the call was not terminated.

In the current release, P-GW terminates the call even if the static rules are not configured and an error-result code is returned in CCA-I with CCFH action set as continue.

Call Termination Without CCR-T During Failure - Behavioral Change

This Diameter-related behavioral change is applicable to all products that use the Gx interface.

In the earlier releases, CCR-T was sent when a permanent failure result code (5xxx result codes) was received and the Disconnect reason was “ims_auth_decision_invalid”.

In the current release, the call is dropped without sending CCR-T when the permanent failure result code (5xxx result codes) is received and the Disconnect reason will be “ims-authorization-failed”.

Case Insensitive Configuration of Diameter Nodes - Behavioral Change

This Diameter-related behavioral change is applicable to all products.

In the earlier releases, the configuration of Diameter nodes and host strings like endpoint name, peer name, host name, realm name, and fqdn were case-sensitive. Hence, it was difficult to handshake with an external node with the name specified in a different case. That is, if a peer is configured as **peer.cisco.com,** it failed to open connections from a peer identifying as **PEER.cisco.com**. Also, configuring endpoints with different cases duplicate the configuration. For example, when configuring endpoints **ep1** and **EP1**, it will assume it to be different and add these separately in the configuration.

In the current release, all the Diameter related node IDs are considered case insensitive. This change applies to both the local configuration and communication with external nodes. When configuring endpoints **s6a-endpoint-mme**, **S6A-endpoint-MME**, **S6A-ENDPOINT-MME**, all these three will be considered the same.

Charging over Gx Feature Licensing Requirements - Behavior Change

This Diameter-related behavioral change is applicable to all products that use Gx interface.

In the earlier releases, there was a separate license for Charging over Gx / Volume Reporting over Gx feature.

in the current release, no specific license is required for Charging over Gx / Volume Reporting over Gx feature. This feature will now be enabled as part of “Policy Interface” license.

Charging Rulebase Name Length in LOSDVs of eG-CDRs and PGW-CDRs

The maximum character length of Charging Rulebase Name field in LOSDVs of eG-CDRs and PGW-CDRs is now configurable. This change is now available in 12.0 and later releases.

In earlier releases, in case of Custom5 or Custom40 dictionaries, the rulebase name used to get trimmed to 16 characters. In other dictionaries the complete rulebase name used to appear in the LOSDVs.

A new CLI command now enables to configure maximum length of the rulebase name between 1 through 63 characters. If configured as 0 (zero), the rulebase name is not trimmed. This new CLI command is available at the context and GTPP group levels.

Diameter Server Selection for Load-balancing

Diameter load balancing implementation maintains a fixed number of servers active at all times for load balancing in case of failures. This can be done by selecting a server with lower weight and adding it to the set of active servers.

Consider the following requirements in the Diameter Endpoint configuration for load balancing:

- Endpoint configuration is needed to specify the minimum number of servers that needs to be active for the service.
- If any one of the servers in the current active group fails, one of the idle servers needs to be selected for servicing the new requests.
- New sessions should be assigned to idle servers with higher weight.
- New session should be assigned to idle servers with lower weight only if
  - The number of active servers are less than the minimum number of servers required for the service
  - Idle servers with higher priority are not available

For more information, refer to the *Command Line Interface Reference*.

eG-CDR in Delimiter Separated ASCII Format

This release supports generating eG-CDRs in delimiter separated ASCII format.

eG-CDRs can be in ASN.1 format or in delimiter-separated ASCII format. Configuring the eG-CDR encoding type is a CLI-configurable parameter. The default encoding type is ASN.1. When configuring the eG-CDR encoding type as ASCII, the delimiter character can be specified as either “:” (colon), “,” (comma), or “|” (pipe). The default delimiter character is “|” (pipe).

Encoding of Bearer-Usage AVP in CCR Messages - Behavioral Change

This Diameter-related behavioral change is applicable to all products that use the Gx interface.

In the earlier releases, the Bearer-Usage AVP was sent in session level CCR-U and CCR-T messages.

In the current releases, the Bearer-Usage AVP is sent only during the establishment of bearers in CCR-I and CCR-U with bearer operation as “Establishment”. This condition is imposed because the session level CCR-U is intended for the entire session and not for a particular bearer.

Encoding of Destination-Host AVP in Initial-Request Messages - Behavioral Change

This Diameter-related behavioral change is applicable to all products that use the S6a interface.

In the earlier releases, the Destination-Host AVP was not sent in session-setup/initial request (first message sent on that interface for that subscriber. This message will vary with different interfaces. For example, CCR-Initial for Gy, ACR-start for Rf, and so on). Also, Destination-Host AVP was not sent in retried requests. For example, CCR-Update failed to be responded by server. The message was retransmitted to alternate server.

In both these scenarios, it is not known which server will respond to the initial/retried message, so the Destination-Realm is encoded but not the Destination-Host. Only after a response for this message is received from one of the hosts present in that realm, the session is considered to be BOUND with that server. Any message sent after this binding will have the Destination-Host AVP encoded.

In the current release, with the CLI command "**`destination-host avp session binding …`** ", if the application has selected one of the servers using application-level commands like peer-select command in case of credit-control or diameter authentication/accounting server command in AAA group, encoding of this AVP in initial/retried request is configurable.

Encoding of Network-Request-Support AVP in CCR Messages - Behavioral Change

This Diameter-related behavioral change is applicable to all products that use the Gx interface.

In the earlier releases, the Network-Request-Support AVP was sent in CCR-T and session level CCR-U messages.

In the current release, if the network-initiated bearer establishment request procedures are not applicable during IP-CAN session establishment, this AVP will not be encoded in CCR-I and in the subsequent messages unless the AVP value is toggled from 1 to 0 and vice-versa.

If the network-initiated procedures are applicable during IP-CAN session establishment, this AVP will be encoded only in the CCR-I and not in the subsequent messages including session level CCRs unless the AVP value is toggled.

Encoding of Offline AVP in CCR Messages - Behavioral Change

This Diameter-related behavioral change is applicable to all products that use the Gx interface.

In the earlier releases, the Offline AVP in Gx CCR-I was sent based on the presence of "billing-action egcdr" OR "billing-action rf" configuration within the charging-action of the ECSv2 rulebase chosen for the Diameter Gx session.

In the current release, the Offline AVP in Gx CCR-I is sent based on the mapping of the Charging-Characteristics-Profile (received in the GTPC Create-PDP-Context-Request) to the Offline AVP (the mapping is CLI configurable in the Policy Control Configuration mode).

Encoding of QoS-Upgrade and QoS-Negotiation AVPs in CCR Messages - Behavioral Change

This Diameter-related behavioral change is applicable to all products that use the Gx interface.

In the earlier releases, the QoS-Upgrade and QoS-Negotiation AVPs were sent in session level updates and in CCR-T message.

In the current release, as the QoS-Upgrade and QoS-Negotiation AVPs are applicable to bearer, these AVPs will no longer be sent in the CCR-U and CCR-T messages.

Encoding of Supported-Features AVP - Behavioral Change

This Diameter-related behavioral change is applicable to all products that use the Gx interface.

In the earlier releases, when Supported-Features AVP was encoded for the following dictionaries, the Vendor-Id AVP under the grouped AVP Supported-Features was sent with "M" bit cleared.

- dpca-custom14
- dpca-custom2
- dpca-custom5
- dpca-custom4
- dpca-custom13
- dpca-custom12
- dpca-custom10

In the current release, when the Supported-Features AVP is encoded for the above mentioned dictionaries, the Vendor-Id AVP under Supported-Features AVP is sent with "M" bit set.

Failure Handling Configuration in IMSA Service - Behavioral Change

This Diameter-related behavioral change is applicable to all products that use the Gx interface.

In the earlier releases, in the case of failure handling, if the CLI command "**`failure-handling cc-request-type …`**" is configured twice under ims-auth-service then the following error message "*Failure: Apply config error*" is displayed. For example, if the failure-handling configured is "X" and if the same failure-handling "X" is applied again then the error message "*Failure: Apply config error*" is displayed.

In the current release, if the same failure-handling configuration is applied under IMSA service then the configuration is accepted as valid and it does not throw any error message.

Failure Result-Code 4010 - Behavioral Change

This Diameter-related behavioral change is applicable to all products.

In the earlier releases, on reception of transient failure result-code 4010 at message/root level by DCCA client, CCR-T was not sent to the OCS server when the DCCA session is terminated.

In the current release, when the failure result-code 4010 is received at message/root level and if CCFH is set to terminate/retry-and-terminate action, then the DCCA session is terminated with CCR-T.

More specifically, for the result-code 4010 received in CCA-U, it is expected to send CCR-T and wait for a response before terminating the DCCA session. For the result-code 4010 in CCA-I, the subscriber session is rejected and CCR-T is sent.

Fire-and-Forget Feature

This release supports the RADIUS Fire-and-Forget feature in conjunction with GGSN for secondary accounting (with different RADIUS accounting group configuration) to the RADIUS servers without expecting acknowledgement from the server, in addition to standard RADIUS accounting. This secondary accounting will be an exact copy of all the standard RADIUS accounting message (RADIUS Start / Interim / Stop) sent to the standard AAA RADIUS server. For this configuring secondary AAA accounting group for the APN is supported.

This release also supports the No-ACK RADIUS Targets feature in conjunction with PDSN and HA for secondary accounting (with different RADIUS accounting group configuration) to the RADIUS servers without expecting the acknowledgement from the server, in addition to standard RADIUS accounting. This secondary accounting will be an exact copy of all the standard RADIUS accounting message (RADIUS Start / Interim / Stop) sent to the standard AAA RADIUS server. For this configuring secondary AAA accounting group for the subscriber template is supported.

For more information, refer to the *ASR 5000 Series Command Line Interface Reference*.

G-CDR Bucket Closure - Behavioral Change

This Diameter-related behavioral change is applicable to all products that use DCCA.

Previous Behavior: The G-CDR buckets are closed on receiving 4010/4012 message level from the OCS when failure-handling is configured as terminate or retry-and-terminate. The final CDR will have Normal closure as the causeForRecordClosing.

New Behavior: The G-CDR buckets are not closed immediately on reception of 4010/4012 at the message level when ccfh is configured as terminate or retry-and-terminate. Instead, some flags are set for the CDRs and when the final CDR is being released due to session termination (initiated by DCCA) the containers will be closed and causeForRecordClosing will be an abnormal release with the appropriate change condition.

Handling of Vendor-specific Application IDs - Behavioral Change

This Diameter-related behavioral change is applicable to all products that use the Gx interface.

In the earlier releases, when the Diameter proxy was not configured, the grouped AVP "Vendor-Specific-Application-Id" in CER/CEA messages contained all the Vendor IDs present in the dictionary file. Hence, if the Gx application used a Customer Specific AVP, this Vendor ID was also added in the Vendor-Id of Vendor-Specific-Application-Id AVP.

In the current release, if **`use-proxy`** is not configured in the Diameter endpoint, the Vendor-Specific-Application-Id AVP in CER/CEA messages will contain only the 3GPP Vendor ID (10415) in the Vendor-Id of the Vendor-Specific-Application-Id AVP.

ICSR Compatibility Between StarOS Versions

The interchassis session recovery (ICSR) feature has been modified to support a greater number of subscribers more efficiently.

Before Release 11.0, the ASR 5000 allocated a AAA session and sub-session for every bearer. Allocating AAA sessions per bearer required great amounts of memory and CPU.

In Release 11.0 and beyond, AAA session handling has been moved from bearer level to call line level. A call-id can have a single AAA session, regardless of the number of bearers; this change allows significant savings in memory when more bearers are activated.

The AAA session handling changes resulted in subsequent changes in the way in which recovery and ICSR work. Therefore, ICSR from StarOS 10.0 or lesser versions will not work when ICSR is attempted to StarOS 11.0 and above. The following table gives a brief overview of different StarOS versions and whether ICSR is supported or not.

Table 1-2 ICSR Compatibility in StarOS Versions

StarOS Version (Active)	StarOS Version (Standby)	ICSR Supported
9.0	9.0	Yes
9.0	10.0	Yes
9.0	11.0	No
9.0	12.0	No
10.0	9.0	Yes
10.0	10.0	Yes
10.0	11.0	No
10.0	12.0	No
11.0	9.0	No
11.0	10.0	No
11.0	11.0	Yes
11.0	12.0	Yes
12.0	9.0	No
12.0	10.0	No
12.0	11.0	Yes
12.0	12.0	Yes

For more information on ICSR, refer to the *Cisco ASR 5000 Series System Administration Guide*.

Increased Attribute Value for 3GPP-IMSI-MCC-MNC - Behavioral Change

This AAA-related behavioral change is applicable only to P-GW.

In the earlier releases, for PGW mediation accounting, the number of digits in 3GPP-IMSI-MCC-MNC AVP was decided based on the MCC and MNC in the PGW service PLMN configuration.

In the current release, the number of digits in the 3GPP-IMSI-MCC-MNC attribute value is purely based on a hardcoded table containing a list of MCCs for which the MNC is of 3 digits.

Note that internally a table is maintained for this, which is used to compare the first three digits of IMSI with entries in the table and check whether there is a match. If yes, the MNC is encoded as three digits (which is the 4th, 5th and 6th digits in IMSI) else it will be encoded as 2 digits (4th and 5th digits of IMSI).

Multiple-Services-Indicator AVP in Diameter CC Requests - Behavioral Change

This Diameter-related behavioral change is applicable to all products that use the Gy interface.

In the earlier releases, Multiple-Services-Indicator AVP was sent in all diameter CC request messages - CCR(I/U/T).

In the current release, Multiple-Services-Indicator AVP will be sent in CCR-Initial message only. This AVP will not be sent in update/terminate requests. This is applicable for all Gy dictionaries.

Monitoring-Key AVP - Behavioral Change

This Diameter-related behavioral change is applicable to all products that use the Gx interface, and all Diameter dictionaries except for the KTF-specific dictionary.

In the earlier releases, PCEF considered the Monitoring-Key AVP as an unsigned integer internally and hence stripped off the insignificant zeroes in the AVP while encoding/decoding it over Gx.

In the current release, the insignificant zeroes are not stripped off while encoding/decoding the Monitoring-Key AVP over Gx.

New Attributes Inclusion in starent-vsa1 Dictionary

In 12.0 and later releases, no new attributes can be added to the **starent-vsa1** dictionary. If there are any new attributes to be added, these can only be added to the **starent** dictionary. For more information, please contact your Cisco account representative.

Notification of Bearer Session Termination During Failover - Behavioral Change

This Diameter-related behavioral change is applicable to GGSN.

In the earlier releases, if in a scenario where there are multiple network initiated bearers and one UE initiated bearer and if only UE initiated bearer is down,

- the PCRF was not notified about the bearer deletion i.e., a CCR-U with bearer operation termination was not sent to the PCRF.
- Also, the "**show ims-authorization sessions full all**" CLI command displayed one IMSA session after the deletion of UE initiated bearer.

In the current release, if UE initiated bearer is down,

- PCRF will be intimated about this bearer deletion i.e., a CCR-U with bearer operation termination will be sent to PCRF. Subsequently, a new IMSA session will be created for one of the existing network initiated bearers (Normally IMSA session will be created ONLY for UE initiated bearers).
- Before receiving the answer (CCA) from PCRF, the "**show ims-authorization sessions full all**" CLI command will show two IMSA sessions.
- After receiving the answer (CCA) from PCRF the "**show ims-authorization sessions full all**" CLI command will show one IMSA session.

Post-processing of Blacklisted Content

Whenever RADIUS/Diameter prepay server blacklists content the packets are generally discarded. To enable redirection of such content, post-processing on blacklisted content is required. With this change, RADIUS/Diameter Credit-Control application will decide on whether to allow post-processing to be enabled or not for the blacklisted content.

In release 12.0, in the ACS Rulebase Configuration Mode, the following configuration is available to enable post-processing priority based rules for content in blacklisted state.

```
post-processing policy { always | not-for-dynamic-discard }
default post-processing policy
```

Release 12.0 onwards "**cca quota-state ...**" and "**cca redirect-indicator ...**" ACS ruledef commands should be used as a post-processing rule. And, "**post-processing policy always**" command should be configured in the ACS Rulebase Configuration Mode for these post-processing rules to be enabled for blacklisted content.

IMPORTANT

In existing deployments, this requires changes to configurations with quota-limit rules for certain features to work.

The following is a sample configuration from existing deployments before this change:

```
configure
  active-charging service service1
    ruledef http_low
      http any-match = TRUE
      cca quota-state = limit-reached
    #exit
    ruledef httpany
      http any-match = TRUE
    #exit
    charging-action standard1
      content-id 1
      cca charging credit
    #exit
    charging-action redirect
      flow action redirect-url http://aoc.com
    #exit
    rulebase base1
      action priority 10 ruledef http_low charging-action redirect
      action priority 30 ruledef httpany charging-action standard1
    #exit
end
```

The following is a sample configuration after this change:

```
configure
  active-charging service service1
    ruledef http_low
      http any-match = TRUE
      cca quota-state = limit-reached
      rule-application post-processing
    #exit
    ruledef httpany
      http any-match = TRUE
    #exit
    charging-action standard1
      content-id 1
      cca charging credit
    #exit
    charging-action redirect
      flow action redirect-url http://aoc.com
    #exit
    rulebase base1
      action priority 30 ruledef httpany charging-action standard1
      post-processing policy always
      post-processing priority 1 ruledef http_low charging-action redirect
    #exit
end
```

If this configuration change is not undertaken, when the content is blacklisted and for any packet that can be redirected and that matches this blacklisted content, then redirection will not happen based on "**`flow action redirect-url`**" command.

Realm-based Routing

In the current release, the Diameter routing logic has been modified to enable routing to destination hosts that are not directly connected to the Diameter clients like GGSN, MME, PGW, and that does not have a route entry configured. Message routing to the host is based on the realm of the host.

For a given session towards a Destination Host, all the messages belonging to the session will be routed through the same peer until the peer is down. If the peer goes down, for the subsequent messages failure handling mechanism will be triggered and the message will be sent using other available peers connected to the destination host.

Rejection of Access Side Update Procedure - Behavioral Change

This Diameter-related change is applicable only for a GnGp call in P-GW.

In the earlier releases, if default bearer QoS/APN AMBR change was reported in CCR-U but not authorized by PCRF, the access side Update PDP context (UPC) request was rejected with GTP_SYSTEM_FAILURE message in case of 3G call on P-GW.

In the current release, if QOS_Change trigger is hit and PCRF does not authorize the QoS, the access side UPC request is not rejected in case of 3G call on PGW.

Sanity Checks for Revalidation-Time AVP - Behavioral Change

This Diameter-related behavioral change is applicable to all products that use the Gx interface.

In the earlier releases, if Revalidation-Time AVP sent in CCA-I message by PCRF fails sanity checks, call is terminated with the Termination-Cause AVP set to the value DIAMETER_BAD_ANSWER (3).

In the current release, the call will continue irrespective of the sanity failure status of Revalidation-Time AVP in the CCA-I message.

Smart Call Home

This release of StarOS incorporates the initial hooks required to support Cisco Smart Call Home (SCM). Smart Call Home is a powerful service capability of Cisco SMARTnet® Service that offers real-time alerts, remediation, and personalized web-based reports on select Cisco devices. Customers and the Technical Assistance Center (TAC) get the information they need to quickly identify and resolve network issues rapidly.

Cisco Smart Call Home enables faster issue resolution and higher network availability by:

- Providing a continuous connection to Cisco that provides monitoring, real-time troubleshooting, alerts, and remediation on select Cisco “call home” enabled devices.
- Automatically generating a Cisco Service Request for severity 1 problems and is sent to the appropriate engineer at TAC.
- Giving the customer greater visibility into network performances through Call Home messages, recommendations, inventory, field notices, security advisories, and End-of-Life notices for select Cisco devices through a Web-based portal.

Smart Call Home will be available as part of a Cisco SMARTnet Service contract. For more information, refer to the Smart Call Home website at: http://www.cisco.com/en/US/products/ps7334/serv_home.html.

Supported-Features AVP - Behavioral Change

This Diameter-related behavior change applies to all products that use 3GPP Rel. 7 Gx dictionaries.

In the earlier releases, if a 3GPP Rel. 7 based dictionary is already configured with **`diameter dictionary dpca-custom4`** command, and then if the **`diameter update-dictionary-avps 3gpp-r9`** command is applied, the Supported-Features AVP was sent with “M” bit set.

[V] [M] Supported-Features:

[M] Vendor-Id: 10415

[V] [M] Feature-List-ID: 1

[V] [M] Feature-List: 2

In the current release, if a 3GPP Rel. 7 based dictionary is already configured with **`diameter dictionary dpca-custom4`** command, and then if the **`diameter update-dictionary-avps 3gpp-r9`** command is applied, the Supported-Features AVP will be sent with “M” bit cleared. All sub AVPs in this grouped AVP will also have 'M' bit cleared.

[V] Supported-Features:

[M] Vendor-Id: 10415

[V] Feature-List-ID: 1

[V] Feature-List: 2

TACACS+ AAA Service Support for Administrative Users

This release supports TACACS+ authentication, authorization and accounting services for ASR 5000 administrative users.

For more information on TACACS+ configuration and maintenance, refer to the *ASR 5000 Series System Administration Guide*, the *ASR 5000 Command Line Interface Reference*, and the *ASR 5000 Statistics and Counters Reference*.

Termination-Cause AVP in CCR-T Request - Behavioral Change

This Diameter-related behavioral change is applicable to all products that use the Gx interface.

In the earlier releases, when the OCS Gy servers are down, then in the CCR-T request message, the Termination-Cause AVP had DIAMETER_LOGOUT as the termination cause.

In the current release, Termination-Cause AVP will have DIAMETER_ADMINISTRATIVE as the termination cause in the CCR-T.

Upgrade Support for 3GPP Release based Dictionary - Behavioral Change

This Diameter-related behavioral change is applicable to all products that use the Gx interface.

In release 12.0, in the Policy Control Configuration mode, the following configuration is available to upgrade any 3GPP release based dictionary to higher version.

`[default | no] diameter update-dictionary-avps {3gpp-r8 | 3gpp-r9}`

Release 12.0 onwards, if a Rel. 7 based dictionary is already configured with **`diameter dictionary dpca-custom4`** command, and then if the **`diameter update-dictionary-avps 3gpp-r9`** command is applied, the Supported-Features AVP with feature bit 1 being set will be sent in the CCR-I to indicate that 3GPP Rel. 9 AVPs are also supported.

This CLI command when configured results in behavioral changes as indicated in the following table.

Possible Upgrade Scenarios	Behavior
3GPP Rel. 7 based dictionary upgraded to 3GPP Rel. 9 For example: **`diameter dictionary dpca-custom4`** **`diameter update-dictionary-avps 3gpp-r9`**	In the CCR-I, Supported-Features AVP will be encoded with value 2 for the Feature-List AVP. [V] [M] Supported-Features: [M] Vendor-Id: 10415 [V] [M] Feature-List-ID: 1 [V] [M] Feature-List: 2 The Feature-List AVP value suggest that it is 3GPP Rel. 9 compliant. But, it is not fully complaint to 3GPP Rel. 9. In the current release, for this upgrade scenario (3GPP Rel. 7 to 3GPP Rel. 9), only volume reporting related AVPs mentioned in the 3GPP Rel. 9 will be supported.
3GPP Rel. 7 based dictionary upgraded to 3GPP Rel. 8 For example: **`diameter dictionary dpca-custom4`** **`diameter update-dictionary-avps 3gpp-r8`**	In the CCR-I, Supported-Features AVP will be encoded with value 1 for the Feature-List AVP. [V] [M] Supported-Features: [M] Vendor-Id: 10415 [V] [M] Feature-List-ID: 1 [V] [M] Feature-List: 1 The Feature-List AVP value suggest that it is 3GPP Rel. 8 compliant. But, it is not fully complaint to 3GPP Rel. 8. In the current release, for this upgrade scenario (3GPP Rel. 7 to 3GPP Rel. 8), none of the features mentioned in 3GPP Rel. 8 will be supported.

Possible Upgrade Scenarios	Behavior
3GPP Rel. 8 based dictionary upgraded to 3GPP Rel. 9 For example: **`diameter dictionary r8-gx-standard`** **`diameter update-dictionary-avps 3gpp-r9`**	In the CCR-I, value for the Feature-List AVP in the Supported-Features AVP will be 2. [V] [M] Supported-Features: [M] Vendor-Id: 10415 [V] [M] Feature-List-ID: 1 [V] [M] Feature-List: 2 The Feature-List AVP value suggest that it is 3GPP Rel. 9 compliant. But, it is not fully complaint to 3GPP Rel. 9. Currently for this upgrade scenario (3GPP Rel. 8 to 3GPP Rel. 9), only volume reporting related AVPs mentioned in 3GPP Rel. 9 will be supported.

Validation of QCI for Default-EPS-Bearer-QoS AVP - Behavioral Change

This Diameter-related behavioral change is applicable to P-GW Rel. 8 Gx interface support.

In the earlier releases, for Default-EPS-Bearer-QoS AVP, the IMSA validation for Quality of service Class Identifier (QCI) range was performed based on standard specifications. The ranges 1–9 and 128–254 were considered valid.

In the current release, the range 1–32 is valid. This change has been implemented to align with the configurable QCI range that the CLI supports.

Vendor-IDs in CER/CEA for STa and S6b Applications - Behavioral Change

This Diameter-related behavioral change is applicable to all products that use the STa and S6b application interfaces.

In the earlier releases, CER/CEA for STa and S6b applications included all the vendor-ids supported by the dictionary in Vendor-ID AVP under Vendor-Specific-Application-ID Grouped AVP. However, per the specification, it should include only 3GPP Vendor-ID (10415) as these are 3GPP specific applications.

In the current release, for the STa and S6b applications, the CER/CEA will have only 10415 (3GPP Vendor-ID) as Vendor-ID AVP value under Vendor-Specific-Application-ID AVP.

Volume Reporting over Gx - Behavioral Changes

The following behavioral changes relate to the Volume Reporting over Gx feature:

- Total threshold level along with uplink/downlink threshold level is treated as an error and only total threshold level is now accepted.
- Enabling and disabling session usage in a single message from PCRF is now supported. This is only if the monitoring key is associated at session level.

- If no new threshold is provided in response for the usage report, monitoring is stopped. Earlier workaround to stop monitoring by providing the Usage-Monitoring-Information AVP but without threshold is now not applicable.
- Monitoring usage based on input/output octet threshold levels is now supported. Usage is reported based on the enabled threshold level. If multiple levels are enabled, usage will be reported on all the enabled levels even if only one of the levels is breached. Monitoring will be stopped on the missing threshold levels in the response for the usage report from PCRF (expected to provide the complete set again if PCRF wants to continue monitoring on the multiple levels enabled earlier).
- Volume or rule information obtained from PCRF is discarded when the subscriber is going down.
- Usage reporting on last rule deactivation using rule deactivation time set by PCRF is now supported.

For more information on Volume Reporting over Gx feature, refer to the *Gx Interface Support* appendix in the administration guide for the product that you are deploying.

Common Features in Release 12.1

This section provides information on new features that are common to products in Release 12.1.

Charging over Gx Feature Licensing Requirements - Behavior Change

This Diameter-related behavioral change is applicable to all products that use Gx interface.

In the earlier releases, there was a separate license for Charging over Gx / Volume Reporting over Gx feature.

in the current release, no specific license is required for Charging over Gx / Volume Reporting over Gx feature. This feature will now be enabled as part of “Policy Interface” license.

Diameter Proxy Capacity Improvement with One Gx Peer - Behavioral Change

This Diameter-related behavioral change is applicable to IPCF.

In the earlier releases, the Diameter proxy in master-slave mode used to do load distribution to all the slave tasks based on peer ID of the incoming session. Thus, all the sessions coming from the same peer were going to the same Diameter proxy.

In the current release, the sessions are distributed across different slaves/worker proxies based on a hash value calculated from the session ID. Thus, all the sessions having the same hash value will go to the same proxy. This eliminates the need at client to have multiple peers to make use of all the proxies at PCRF.

Protocol and Session Handling - Behavioral Change

This AAA-related behavioral change is applicable to IPCF.

In the earlier releases, in case of SNR-Registration profile fetch failure due to SPRMGR crash/messenger loss, PCC Session was hanging in SPR-Wait state. This was happening since no session setup timer was present at IPCF.

In the current release, IPCF supports a timer called setup timer. This timer is started during every PCC Session creation which is triggered through CCR-Initial message over Gx interface. Setup timer is always started with a value of 60 seconds which is not configurable. When SPR Profile information/Fetch Error information for SNR-register does not arrive at PCCMGR within 60 seconds, PCC session is deleted with disconnect reason "Session-Setup-Timeout".

In case PCCMGR receives SPR profile information within 60 seconds of placing the request, the setup timer is stopped and never restarted again. Session-setup timer is stopped even when SPRMGR explicitly communicates profile fetch error/SSC message timeout to PCCMGR through messenger.

Common Features in Release 12.2

This section provides information on new features that are common to products in Release 12.2.

Auth-Application-Id AVP Value for Standard S6b Dictionary - Behavioral Change

This Diameter-related behavioral change is applicable to all products that use the S6b interface.

In the earlier releases, Auth-Application-Id AVP was sent as 16777999 in CER/AAA messages for the standard dictionary "aaa-custom14" used for S6b interface.

In the current release, per the 3GPP TS 29.273 standard, the Auth-Application-Id AVP will be sent as 16777272 for the S6b standard dictionary.

CCR-U with Usage Reports - Behavioral Change

This Diameter-related behavioral change is applicable to all products that use the Gx interface.

In the earlier releases, CCR-U with accumulated usage report was sent for immediate reporting request or explicit usage monitoring disable request by PCRF without any new threshold in CCA-U, which corresponds to the usage report in previous CCR-U for the same monitoring keys.

In the current release, the usage monitoring information instances containing Usage-Monitoring-Report / Usage-Monitoring-Support are not forwarded if the usage for the corresponding monitoring keys have been reported in CCR-U. This avoids the duplication of sending another CCR-U with zero usage when no new threshold is provided by PCRF for the corresponding usage report.

Change in Diameter AVP Flags - Behavior Change

This Diameter-related behavioral change is applicable to PDSN, MME and SGSN.

Previous Behavior: The M bit was not set for the following AVPs:

- RAT-Type
- Priority-Level
- Pre-emption-Capability
- Pre-emption-Vulnerability

New Behavior: The flag value for the following AVPs in the CCR messages has been changed from V to M:

- RAT-Type - included in standard PDSN Ty and Ty-plus dictionaries

- Priority-Level - included in Diameter HSS custom1 and standard dictionaries for MME and SGSN products
- Pre-emption-Capability - included in Diameter HSS custom1 and standard dictionaries for MME and SGSN products
- Pre-emption-Vulnerability - included in Diameter HSS custom1 and standard dictionaries for MME and SGSN products

Change in Error Handling at GGSN

This Diameter-related behavioral change is applicable to GGSN.

In the earlier releases, call was terminated when GBR QoS was requested and non-GBR QoS was authorized and sent in CCA request message from PCRF.

In the current release, call is not terminated now when GBR QoS is requested and non-GBR QoS is authorized.

Change in Value for Termination-Cause AVP During Call Termination - Behavioral Change

This Diameter-related behavioral change is applicable to all products which use Gy interface.

In the earlier releases, on clearing the call with the **`clear subscribers all`** command, DIAMETER_LOGOUT was sent as Termination-Cause to the OCS in CCR-T.

In the current release, on clearing the call DIAMETER_ADMINISTRATIVE is sent as Termination-Cause to the OCS in CCR-T.

Charging over Gx Feature Licensing Requirements - Behavior Change

This Diameter-related behavioral change is applicable to all products that use Gx interface.

In the earlier releases, there was a separate license for Charging over Gx / Volume Reporting over Gx feature.

in the current release, no specific license is required for Charging over Gx / Volume Reporting over Gx feature. This feature will now be enabled as part of “Policy Interface” license.

Cleanup of Dedicated Bearers on Rulebase Change from CoA

This Diameter-related behavioral change is applicable to all products which use Gx interface.

In the earlier releases, ECS displayed the bearers without rules and used the same bearer to update in case of same predef rules reinstallation. That is, ECS session used to lump around without rules and get updated with new rules resulting in the dedicated bearer session being left uncleared when the rulebase is changed via CoA.

In the current release, rulebase change will clear off Gx installed rules and dedicated bearers. ECS will recreate bearers based on what is sent from Gx.

Dynamic Route - Behavioral Change

This Diameter-related behavioral change is applicable to GGSN, HSGW, PDG, PDIF, P-GW, SCSCF/ICSCF, S-GW.

Previous Behavior: A dynamic route entry was deleted immediately after the expiry of route.

New Behavior: If there are multiple dynamic routes (multipath routes) for a host then either all should exist or none should exist. That is, a multipath dynamic route entry will be deleted only if all the multipath routes are expired. Because of this change the cli command, **`show diameter route table`** will show dynamic route entries with negative expiry value.

Encoding of 3GPP-SGSN-MCC-MNC AVP - Behavioral Change

This Diameter-related behavioral change is applicable to all products that use Gx interface.

In the earlier releases, for 3GPP-SGSN-MCC-MNC AVP, the mandatory (M) bit was reset thereby causing Gx CCR-I to be rejected.

In the current release, the M bit will be set for the 3GPP-SGSN-MCC-MNC AVP.

Encoding of Acct-Application-Id AVP in CER/CEA - Behavioral Change

This behavioral change to aaa-custom5 dictionary is customer specific. For more information contact your local sales representative.

In the earlier releases, CER/CEA received without Acct-Application-Id AVP was considered as an error due to the fact that the Diameter connections were closed at that time.

In the current release, Diameter connections will remain active even when CEA is received without Acct-Application-Id AVP. Hence, CER/CEA messages received without Acct-Application-Id AVP are no longer considered as an error.

Encoding of Allocation-Retention-Priority AVP - Behavioral Change

This Diameter-related behavioral change is applicable to all products that use the Gx interface.

In the earlier releases, the Allocation-Retention-Priority (ARP) AVP and all sub AVPs were sent without M bit set according to 8.7.0 version of 3GPP standard spec, TS 29.212.

In the current release, the ARP AVP and all sub AVPs are being sent with M bit set as per the 3GPP standard spec TS 29.212, version 8.6.0.

Encoding of AN-GW-Address AVP - Behavioral Change

This Diameter-related behavioral change is applicable to all products that use Gxa interface.

Previous Behavior: The AN-GW-Address AVP was not sent in the CCR-I and RAA messages.

New Behavior: The AN-GW-Address AVP is now sent in the CCA-I and RAA messages for Gxa 3GPP2 standard dictionary.

Encoding of Gx Specific Diameter AVPs - Behavioral Change

This Diameter-related behavioral change is applicable to all products that use the Gx interface, and HSGW that use the Gxa interface.

In the earlier releases, “M” bit was set for the following Gx-specific Diameter AVPs violating the standard spec, 3GPP TS 29.212:

- Allocation-Retention-Priority
- AN-GW-Address
- APN-Aggregate-Max-Bitrate-DL
- APN-Aggregate-Max-Bitrate-UL
- Charging-Correlation-Indicator
- CoA-IP-Address
- CoA-Information
- Default-EPS-Bearer-QoS
- Event-Report-Indication
- Flow-Information
- Flow-Label
- Packet-Filter-Content
- Packet-Filter-Identifier
- Packet-Filter-Information
- Packet-Filter-Operation
- Pre-emption-Capability
- Pre-emption-Vulnerability
- Priority-Level
- RAT-Type
- Resource-Allocation-Notification

- Security-Parameter-Index
- Tunnel-Header-Filter
- Tunnel-Header-Length
- Tunnel-Information

In the current release, the “M” bit is removed for these AVPs. The Diameter incoming message parsing now takes care of the absence of the “M” bit in these AVPs correctly.

Encoding of Packet-Filter-Content and Precedence AVPs - Behavioral Change

This Diameter-related behavioral change is applicable to all products that use Gxa interface.

Previous Behavior: The Packet-Filter-Content and Precedence AVPs were not sent in the update request message.

New Behavior: The Packet-Filter-Content and Precedence AVPs are now sent in the CCR-U message for Gxa 3GPP2 standard dictionary.

Encoding of Supported-Features AVP in CCR-I - Behavioral Change

This Diameter-related behavioral change is applicable to all products that use the 3GPP Rel. 8 Gx dictionaries “r8-gx-standard” and “dpca-custom17”.

In the earlier releases, the Supported-Features AVP was sent in CCR-I message with “M” bit cleared.

[V] Supported-Features:

[M] Vendor-Id: 10415

[V] Feature-List-ID: 1

[V] Feature-List: 1

In the current release, the Supported-Features AVP is sent in the CCR-I message with “M” bit set.

[V] [M] Supported-Features:

[M] Vendor-Id: 10415

[V] Feature-List-ID: 1

[V] Feature-List: 1

Encoding of User-Name AVP - Behavioral Change

This Diameter-related behavioral change is applicable to HSGW.

In the earlier releases, User-Name AVP was not included in RAA message for standard dictionary.

In the current release, per the standard spec 3GPP 29.273, the User-Name AVP will be included in RAA message for standard dictionary.

Encoding of Termination-Cause AVP - Behavioral Change

This Diameter-related behavioral change is applicable to all products that use Gxa interface.

Previous Behavior: The Termination-Cause AVP was not sent in the Credit-Control-Request-Termination (CCR-T) message.

New Behavior: The Termination-Cause AVP is now sent in the CCR-T message for Gxa 3GPP2 standard dictionary.

Error Code Handling in Diameter for Error Code 5002 (Unknown Session ID) - Behavioral Change

This behavioral change to dcca-custom12 and dcca-custom13 dictionaries is customer specific. For more information contact your local sales representative.

When the OCS is unreachable or returns certain failure error-result codes, PCEF should assign default volume quota or time and retry the OCS server when this quota exhausts or time expires. In the earlier releases, the PCEF entered assume positive state when receiving the following error-result codes - UNABLE_TO_DELIVER (3002), UNABLE_TOO_BUSY (3004), ELECTION_LOST (4003), and Permanent failures (5000-5999).

In the current release, if the PCEF receives the result code 5002, it will disconnect the session and will not enter/re-enter assume positive state. The PCEF will initiate a new session with a CCR-I. No interim data will be reported at this point; the session will continue as a standard new Gy session.

MSISDN Prefix/Suffix/Range Based OCS/IN Peer Selection

This feature enables configuring both IMSI-based and MSISDN-based values under a particular credit control group. With this feature enabled, you can select appropriate Diameter peer based on the configured Mobile Station International Subscriber Directory Number (MSISDN) prefix/suffix/range value. Default peer will be selected when the MSISDN value does not match any of the configured range. If the default peer is not configured, one of the peers in Diameter endpoints will be chosen.

Output of Session Active Counter in show ims-authorization servers ims-auth-service Command - Behavioral Change

This Diameter-related behavioral change is applicable to all products that use the Gx interface.

In the earlier releases, the counter "**Sessions Active**" under the "**`show ims-authorization servers ims-auth-service <service_name>`**" CLI command was used to indicate the total number of sessions that were referencing the server as active.

In the current release, this counter provides the count of sessions that are referencing this server as either active or standby.

RAT-Type - Behavioral Change

This Diameter-related behavioral change is applicable to all products which use Gx interface.

In 12.1 and earlier releases, the RAT-Type AVP was marked as Mandatory.

In 12.2 and later releases, the RAT-Type is marked as NOT Mandatory in order to be compliant with the standard spec 3GPP TS 29.212 v8.6.0. That is, the M flag for the RAT-Type has changed from 1 to 0 in Gx CCR message.

Static Rules for Bearers

This Diameter-related behavioral change is applicable only to P-GW.

In the earlier releases, DCCA was assuming that static rules defined in a rulebase were applicable for all bearers.

In the current release, the static rules defined in a rulebase are applied only to default bearers.

The following changes have been made in the DCCA routines to check if DCCA needs to be enabled for a session:

- Default bearers — Check for Credit Control configuration in all static rules in the rulebase. Also check if Credit Control requirements of all predefined and dynamic rules have been installed.
- Dedicated bearers — Check for Credit Control requirements of all predefined and dynamic rules have been installed. The charging-actions of the installed predefined and dynamic rules decide whether DCCA needs to be enabled.

Support for New AAA Thresholds

In this release, the following new thresholds can be configured for generating alarms or alerts based on the archival queue percentage of AAA accounting messages.

- threshold aaa-acct-archive-queue-size1
- threshold aaa-acct-archive-queue-size2
- threshold aaa-acct-archive-queue-size3

Termination of IP CAN Session - Behavioral Change

This Diameter-related behavioral change is applicable to all products that use the Gx interface.

In the earlier releases, IP CAN session was terminated on receiving an experimental result code of range 5xxx in CCA-Update request message.

In the current release, when experimental-result-code of range 5xxx is received, the Diameter peer is notified of the failure and the IP CAN session is no longer terminated.

Threshold-based Session Usage Reporting over Gx - Behavioral Change

This Diameter-related behavioral change is applicable to all products that use the Gx interface.

In the earlier releases, the session level and rule level usage was reported over the Gx interface only when the volume/time threshold is breached.

In the current release, even if the volume/time threshold is reached, the session level usage is reported over Gx.

ADC Features in Release 12.0

This section provides information on new Application Detection and Control (ADC) features in Release 12.0.

P2P Protocols Detection Support

This release now supports the detection of the following P2P protocols:

- Blackberry
- Gmail
- iTunes
- MySpace
- TeamViewer
- Twitter
- Viber

For more information, please refer the *Application and Detection Control Administration Guide*.

Video Detection Support

The system now supports video detection for the following P2P protocols:

- Gtalk

- Oscar
- Yahoo

For more information, please refer the *Application and Detection Control Administration Guide*.

ADC Features in Release 12.2

This section provides information on new Application Detection and Control (ADC) features in Release 12.2.

P2P Protocols Detection Support

This release now supports the detection of the following P2P protocols:

- AntsP2P
- IMO
- MyPeople
- Netmotion
- OGG
- OpenVPN
- Quicktime
- RDT
- Scydo
- Spotify
- Tango
- TunnelVoice — only detection
- Ultrabac
- Usenet
- WhatsApp

IMPORTANT

The Scydo and WhatsApp protocols are new in 9.0 and later releases.

For more information, please refer the *Application Detection and Control Administration Guide*.

Video Detection Support

The system now supports video detection for the P2P protocol - Meebo.

For more information, please refer the *Application Detection and Control Administration Guide*.

ASN GW Features in Release 12.0

This section provides information for new features in the ASN GW Service in Release12.0

WiMAX HA and ASN-GW have been enhanced to support profile-based hotlining as per WiMAX Forum™ Network Architecture, NGW 1.5 specification. See Interface Changes for additional information.

Support for 802.1P Marking

802.1p marking is now supported on ASN-GW with or without Ethernet CS support. See Interface Changes for additional information.

Support for IP 5-Tuple Flow-Based Pre-Paid Accounting

Support has been added for IP 5-tuple flow-based prepaid accounting using ECSv2 rulebase configuration support for WiMAX, ASN-GW and HA calls.

Also added Hotlining support for IP 5-tuple flow-based prepaid call sand postpaid sessions on WiMAX, HA and ASN-GW.

Single DCCA Session Support

ASN-GW now supports a single DCCA session for all the bearers in an IP-CAN Session. See Interface Changes for additional information.

Device ID (MAC Address) Support for WiMAX HA MIPv4 Calls

Device ID extension support has been implemented the following items:

- Device ID extension support for MAC address in PMIPv4
- Hold timer functionality based on MAC address.
- Callgen-FA support for MAC address (device id) extension
- MAC address inclusion in log messages
- Session recovery related changes for MAC address
- show/clear commands with mac-address option

See Interface Changes for additional information.

Payload Header Suppression Support Feature

Added and modified CLI commands to support PHS for WiMax Calls. See Interface Changes for details.

WiMAX HA: Accept MIP Call Without FA-HA AE

Added and modified CLI commands to support PHS for WiMax Calls. See Interface Changes for details.Feature

Added a CLI command option for fa-ha spi config on HA to address the following requirements:

- FA-HA AE is configured as “enabled” with specific range of FA addresses.
- FA-HA AE is configured as “disabled” with specific range of FA addresses

The following CLI command configures these options:

fa-ha-spi remote-address <ip_address> spi-number <spinumber> secret <secret > [allow-fa-ha-auth-extension | disallow-fa-ha-auth-extension]

See Interface Changes for additional information.

New Dictionary for Specific Set of AAA Attributes

A new, HA-specific dictionary has been added as “custom53”. This dictionary contains a specific set of UQ Communications (UQC) AAA attributes.

RADIUS Test Frame Sent According to UQC AAA Dictionary

The ASN-GW can now send the RADIUS test frame (Auth Req and Acct Req) with the exact attribute set identified for the UQC dictionary.

WiMAX Hotlining for Post Paid Sessions

The following features have been added in this release to support WiMAX hotlining:

- IP 5-tuple [Source IP, Destination IP, Source Port, Destination Port, Protocol] flow-based prepaid accounting using ECSv2 rulebase configuration for WiMAX ASN-GW and HA calls.
- Hotlining support for the IP 5-tuple flow-based prepaid calls.
- Hotlining support for postpaid sessions on WiMAX HA and ASN-GW. A session can be hotlined either at the beginning or middle of the session.

Location Based Services Support

For reporting BS-ID based on event triggers such as handover, idle mode entry and exit only

The following changes were done to implement this functionality:

- Idle Mode Entry – If asn-policy idle-mode is enabled, then Interim-Update will be sent with the BSID and WiMAX-Idle-Mode-Transition as “Idle”.
- Idle Mode Exit – If asn-policy idle-mode is enabled, then Interim-Update will be sent with the BSID and WiMAX-Idle-Mode-Transition as “Not Idle”.

- Location Update – If asn-policy notification-handoff is enabled, the Interim-Update will be sent with the BSID and SN-Handoff-Indicator as “Location-Update”.
- Handoff –If asn-policy notification-handoff is enabled, the Interim-Update will be sent with the BSID and SN-Handoff-Indicator as “Active-Handoff”.
- Interim when the call is Idle – During the Idle-Mode Entry, the Interim will not be sent until the Idle-Mode Exit or Location Update.

MPLS VRF Support

MPLS VRF Support for ASNGW service has been implemented.

Content Filtering Features in Release 12.0

This section provides information on new Content Filtering features in Release 12.0.

None for this release.

ECS Features in Release 12.0

This section provides information on new Enhanced Charging Service (ECS) features in Release 12.0.

None for this release.

ECS Features in Release 12.2

This section provides information on new Enhanced Charging Service (ECS) features in Release 12.2.

Charging Rulebase Name Selection - Behavior Change

In 12.0 and earlier releases, if multiple Charging-Rule-Base-Name AVP are received from the PCRF, the "last" rulebase is selected and applied to the call. In early 12.2 releases, the "first" rulebase was being selected.

To maintain a uniform behavior, in later 12.2 releases also the "last" rulebase will be selected by default.

In cases where the "first" rulebase has to be selected, in the **`policy-control charging-rule-base-name`** CLI command a new command option has been introduced to enable that. For more information, in the *Configuration Management* chapter see the **`policy-control charging-rule-base-name`** CLI command.

Content ID and Service ID Configurable Limits in CLI

In 12.1 and earlier releases, and in early 12.2 releases, in the CLI the maximum configurable value for content-id and service-identifier was 65535 (maximum 16 bit value). Now the maximum configurable value is 2147483647 (maximum 31 bit value).

The content-id and service-identifier keywords in the following commands are affected:

ACS Charging Action configuration Mode

content-id *1..2147483647*

service-identifier *1..2147483647*

ACS Ruledef Configuration Mode

if-protocol http content-id *1..2147483647*

if-protocol wsp-connection-less content-id *1..2147483647*

if-protocol wsp-connection-oriented content-id *1..2147483647*

ACS Rulebase Configuration Mode

cca quota holding-time *1..4000000000* **content-id** *1..2147483647*

cca quota time-duration algorithm consumed-time *1..4294967295* **[content-id** *1..2147483647* **]**

cca quota time-duration algorithm continuous-time-periods *1..4294967295* **[content-id** *1..2147483647* **]**

cca quota time-duration algorithm parking-meter *1..4294967295* **[content-id** *1..2147483647* **]**

DNS Snooping

The DNS Snooping feature enables a set of IP rules to be installed based on the response from a DNS query. The rule in this case contains a fully qualified domain name (for example, m.google.com) or its segment (for example, google) and a switch that causes the domain to be resolved to a set of IP addresses. The rules installed are thus IP rules. Any actions specified in the domain rule are inherited by the resulting IP rules.

In the 12.2 release, the DNS Snooping feature is supported only on the GGSN and P-GW.

For more information, refer to the *Enhanced Charging Services Administration Guide*.

Static ECS-specific Memory Threshold

Each SessMgr has some memory dimensioned based on system requirements. ECS has an internal threshold at ~90% of this memory after which it bumps up effective call credits to maximum and this causes silent rejects.

- It is capped at a magic number not allowing the SessMgr to use its entire memory.
- Silent rejects are done even if there is system memory available. Silent in the sense not known unless someone is watching the logs (e.g. no alarms).

- It delays the system to recover from memory leaks by capping the calls. Without ECS, SessMgrs would eventually go to WARN, raise alarms. They can then bloat as much as there is available system memory.

In earlier releases, at approximately 90% CPU utilization, SessMgrs would start rejecting calls with SessMgr event ID 10018.

In this release, this limit is bumped up to ~1.25X. Note that the normal behavior is that SessMgrs reject calls at 120%, independent of ECS. SessMgrs will be able to go up to and over their dimensioned maximum capacity independent of ECS.

Tethering Detection Feature

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

In the 12.2 release, the Tethering Detection feature is supported only on the GGSN.

For more information, refer to the *Enhanced Charging Services Administration Guide*.

Tethering Detection - OS Fingerprint Generation - Behavior Change

Previous Behavior: In earlier 12.2 releases, OS fingerprint generation for all MS-initiated TCP flows on a subscriber call happened irrespective of whether or not the Tethering Detection feature is configured in the rulebase for that subscriber. Therefore the field “tcp-os-signature” was available for export in various types of EDRs independent of the tethering-detection rulebase configuration.

New Behavior: OS fingerprint generation for all MS-initiated TCP flows on a subscriber call will now take place only if the Tethering Detection feature is configured in the rulebase for that subscriber. Therefore, the field “tcp-os-signature” is available for export in various types of EDRs depending on whether or not the “tethering-detection” CLI command is configured in the rulebase.

If the “tethering-detection” CLI command is absent in the rulebase configured for a particular subscriber, and if “tcp-os-signature” field is configured in an EDR format for the EDR generated for the same subscriber, then the “tcp-os-signature” field in the EDR entry in csv file generated is left blank.

Impact: If you want to extract “tcp-os-signature” using EDRs, you must configure “tethering-detection” CLI command in the rulebase.

Tethering Detection - Database File Location - Behavior Change

The directory path to store Tethering Detection databases has changed.

Previous Behavior: In earlier 12.2 releases, the path to store the Tethering Detection database files was “/mnt/hd-raid/data/databases/”.

New Behavior: Now the path to store the tethering database files is “/hd-raid/databases/”.

ESS Features in Release 12.0

This section provides information on new L-ESS features in Release 12.0.

None for this release.

Firewall Features in Release 12.0

This section provides information on new Stateful Firewall features in Release 12.0.

IPv6 and ICMPv6 Firewall Support

This release provides support for IPv6 and ICMPv6 Firewall. IPv6 Firewall supports the following features:

- Enabling/Disabling IPv6 Firewall: The configuration can be used to enable or disable IPv6 Firewall for subscribers. IPv4 and IPv6 Firewall can be enabled or disabled separately.
- IPv6 Header checks: Firewall performs the following header checks to ensure the integrity of an IPv6 packet. IPv6 packets with unknown extension headers will not be dropped by Firewall; such packets will be allowed by Firewall.
  - Limiting extension headers
  - Hop-by-hop Options filtering: The Hop-by-Hop options will be parsed only if any of the Hop-by-Hop dos protections is enabled.
  - Destination Options filtering
  - Router Header filtering
  - Fragment Header filtering
- IPv6 Host Pool: Host pools are enhanced to support IPv6 addresses and address ranges.
- IPv6 Rule-match: Stateful Firewall access ruledefs are enhanced to support IPv6 addresses and other parameters like IP version and ICMPv6 protocol.
- IPv6 Recovery: Stateful Firewall supports IPv6 flow recovery similar to IPv4 flows with the existing flow-recovery CLI being applicable to IPv6 flows also.
- ALG support: Firewall supports IPv6 traffic for ALGs - FTP, RTSP, PPTP, and TFTP.
- Existing DOS protection features enabled for IPv6.
- Malformity check enhanced for IPv6.
- TCP Stateful processing enhanced for IPv6 packets.

For more information, please refer the *Personal Stateful Firewall Administration Guide* and *Command Line Interface Reference*.

FNG Features in Release 12.0

The Femto Network Gateway is a new product in Release 12.0.

For information about the Femto Network Gateway, see the *Femto Network Gateway Administration Guide*.

GGSN Features in Release 12.0

This section provides information on new GGSN features in Release 12.0.

QoS Parameter ARP Setting via Gx Interface

GGSN controls the assignment of different radio interface QoS priorities (gold/silver/bronze) via the PCRF Gx interface during PDP context setup (CCR/CCA-I). This is performed using the Allocation Retention Priority (ARP) parameter (AVP code 1034) as specified in 3GPP TS 29.212, with values = 0-3; ARP values from the PCRF other than 0-3 are ignored. During PDP context setup the PCRF returns the ARP value in CCA-I and this ARP is then assigned/negotiated with the SGSN and RNC.

Charging Rulebase Name in LOSDV is Configurable

The maximum length of the charging rulebase name in List of Service Data Volumes (LOSDV) of eG-CDRs can be trimmed now with the inclusion of a new command "`gtpp egcdr charging-rulebase-name-max-char-length`". With this new command, user will have flexibility to decide the length of charging rulebase name. The user need to specify the rulebase name length explicitly between 1 to 63 in LOSDV to use this feature. In case zero is specified, the charging rulebase name would not be trimmed.

For more information, refer to the *Context Configuration Mode Commands* chapter of the *Command LIne Interface Reference Guide*.

GGSN Features in Release 12.2

This section provides information on new GGSN features in Release 12.2.

CLI Support for RAI/SAI/CGI CDR Triggers

Previous Behavior

ULI-Change is a record closing condition in Release 7 and Release 8 as per the standards. Due to this behavior, the Custom 19/24 dictionaries closed the eG-CDR containers if ULI-change was observed at GGSN. Also there was no CLI control to suppress this trigger if a customer (telecom operator) did not want to implement this behavior.

New Behavior

A new option "`uli-change`" has been included in the existing CLI "`gtpp trigger`" to control the earlier behavior. By default it is enabled. If the trigger is disabled, any subsequent ULI change received at GGSN will not be treated as a trigger to close the

container. Also irrespective of the current ULI of the session, always the first ULI received at the time of call connect will be present in the CDR.

The newly introduced CLI control has no dependence on dictionary. It is effective on all the dictionaries that support ULI-change trigger.

Enhanced S6b Support

S6b is an optional Diameter protocol-based interface over which the GGSN communicates with 3G AAA/HSS in LTE/SAE network for subscriber authorization.

S6b interface has ability to pull SGSN-MCC-MNC from either GTP or AAA-I and send to OCS. When customer roams into GSM environment, OCS needs location information for online charging and metering. 3GPP-SGSN-MCC-MNC AVP and Location Information AVP are defined in Gy and can be used to identify customer location. With this feature, the GGSN collects the value of SGSN-MCC-MNC from the S6b AAA message, so that it can be available to OCS through Gy interface while passing CCR and CCA messages.

From Release 12.2 onwards, the S6b interface has been enhanced to pass on the UE assigned IPv6 address (IPv6 prefix and IPv6 interface ID) to the AAA server. S6b interface also has support for Framed-IPv6-Pool, Framed IP Pool, and served party IP address AVPs based IP allocation. With this support, based on the Pool name and APN name received from AAA server, the selection of a particular IP pool from the configuration is made for assigning the IP address.

GGSN Session License Counting

Previous Behavior

Session credits and session license were counted for both primary and secondary PDP contexts of GGSN call.

New Behavior

Session credits and session license are counted only for primary PDP context of GGSN call.

GTP-U Sequence Number

CLI command added to enable/disable addition of the sequence number to every GTP-U packet coming from Gi interface and going towards Gn/Gp interface. If GTP-U packets are received out of sequence, sequence numbers would allow the packets to be recorded.

IPv4v6 Type PDP Support

GGSN now supports IPv4v6 type PDP from release 12.2 onwards. With this support, on single PDP context, both IPv4 and IPv6 user plane can run simultaneously according to 3GPP TS 23.060 V9.8.0 specification.

Lawful Intercept

TCP Proxy Support

TCP Proxy support is now available for Lawful Intercept on the GGSN. Contact your local Cisco sales representative for additional information.

Notification of Modification/Deletion of LI Target Provision

The GGSN supports the sending of a notification to LI administrators when an existing LI target provision has been modified or deleted. Contact your local Cisco sales representative for additional information.

Rf Interface Support

Rf interface enables offline accounting functions on the GGSN in accordance with the 3GPP Release 8 specifications. The charging data information is recorded at the GGSN for each mobile subscriber UE pertaining to the radio network usage. Due to the transfer of charging information to GGSN, the services being rendered are not affected in real time.

The offline charging functionality is based on the network elements that report the accounting information via different type of messages which trigger the charging generation. Following diameter accounting requests are sent from the network elements to the charging data function (CDF) to achieve this reporting:

- START
- INTERIM
- STOP
- EVENT

HA Features in Release 12.0

This section provides information on new Home Agent (HA) features in Release 12.0.

None for this release.

HNB-Gateway Features in Release 12.1

This section provides information on new features supported on HNB-Gateway (HNB-GW) in Release 12.1.

Multiple MSC Selection without Iu-Flex

In this release multiple MSC selection without Iu-Flex functionality for HNB-GW service is supported.

Support for multiple MSC selection in a CS core network is provided with this feature support.

HNBGW can connect to multiple MSC and SGSN through Iu-Flex or LAC mapping. This feature implements the multiple MSC selection using LAC.

For this support the HNB-GW uses HNBs LAC, received during registration procedure in HNB_REGISTER_REQUEST message, to distribute RANAP-Initial UE message to an MSC. It maps the LAC with MSC point code and a set of LACs configured for each MSC, connected to the HNB-GW.

In the HNBGW, to select an MSC based on the LAC the following algorithm is used:

- If both Iu-Flex and LACs are configured for a MSC, then Iu-Flex is used to select a MSC.
- If only Iu-Flex is configured then Iu-Flex is used for selecting MSC.
- If only LACs are configured then MSC is selected using LAC from HNB.
- If both Iu-Flex and LACs are not configured in the HNBGW, it selects default MSC.

For more information on HNB-GW, refer the *3G Home NodeB Gateway Administration Guide*.

HSGW Features in Release 12.0

This section provides information on new features supported on HRPD Serving Gateway (HSGW) in Release 12.0.

None for this release.

HSGW Features in Release 12.2

This section provides information on new features that pertain to the HRPD Serving Gateway (HSGW) supporting eHRPD network services in Release 12.2. Additional information on these features can be found in the *Cisco ASR 5000 HRPD Serving Gateway Administration Guide* and the *Cisco ASR 5000 Series Command Line Interface Reference.*

AN-GW-Address AVP Missed in CCR-I for Dictionary gxa-3gpp2-standard

Previous Behavior

The AN-GW-Address was not sent in the CCR-I and RAA messages.

New Behavior

Now, the AN-GW-Address AVP is sent in the CCA-I and RAA messages.

AVPs Missed Under Packet-Filter-Information Group AVP in CCR-U for gxa-3gpp2-standard

Previous Behavior

The AVPs Packet-Filter-Content and Precedence were not being sent in the update request.

New Behavior

Now, the AVPs Packet-Filter-Content and Precedence are sent in the CCR-U message.

GTP-U Sequence Number

CLI command added to enable/disable addition of the sequence number to every GTP-U packet coming from Gi interface and going towards Gn/Gp interface. If GTP-U packets are received out of sequence, sequence numbers would allow the packets to be recorded.

Gxa - Behavioral Changes

Default EPS Bearer QoS

Default EPS Bearer QoS was not supported in Gxa messages in earlier releases. Support has been added in CCR/CCA/RAR messages.

CCR

In case of Default EPS Bearer QoS, the value received from STA in EPS_SUBSCRIBED_QOS_PROFILE will be passed on in CCR-I to PCRF.

CCA/RAR

PCRF is supposed to respond in CCA/RAR with QCI 9 for Default Bearer. If HSGW receives a value other than 9, a log is printed. HSGW does **not** terminate the call in such cases.

Event Trigger

Event-Trigger related AVPs were not included in RAA when RAR with Event Trigger was received. Support has been added in RAA messages.

The new behavior is as follows.

- For BSID Change event trigger
  - RAR with event trigger set-> Include the current applicable values.
  - RAR with event trigger not set ->Include the current applicable values if the value has changed. Do not include the AVP, if the value has not changed.
- For all other event triggers
  - RAR with event trigger set ->Include the current applicable values.
  - RAR with event trigger not set -> Do not include the event-trigger-related AVP(s).

Flow-Information AVP

Flow-Information AVP was not supported inside QoS-Rule-Definition in Gxa messages. Support has been added in CCA/RAR messages.

HSGW supports parsing of parameters inside Flow-Information AVP.

Resource Modification Request

Event trigger Resource Modification Request will be triggered when a Resource Modification Request is triggered from UE. Earlier event triggers QoS Change/TFT Change were used for the same.

The event trigger Resource Modification Request need not be turned on from PCRF; it is enabled by default.

Session-Linking-Indicator

Session-Linking-Indicator was not supported in Gxa messages in earlier releases. Support has been added in CCR messages.

This AVP is included only in CCR-Initial messages.

- CCR-I sent as a result of PDN Connect will have the value SESSION_LINKING_DEFERRED.
- CCR-I sent as a result of BBERF Relocation will have the value SESSION_LINKING_IMMEDIATE

Supported-Features AVP

Supported-Features AVP was not supported in Gxa messages in earlier releases. Support has been added in CCR/CCA messages.

HSGW shall set the Supported-Features AVP to Release 9 to indicate compliance to Rel 9. HSGW does not terminate the session if PCRF advertises release 8 support.

Gxa: SM Support for New Parameters in QoS Rule Definition

QoS Rule Definition can contain Flow Information; SM supports handling these new AVPs.

In case of Gx, these parameters are sent as part of the filters to UE and are used for rule matching. Packet Filter ID needs to be stored for all rules which are configured by PCRF as a result of UE-requested resource modification process. These filter IDs need to be used as a key between PCRF and BBERF for any further modification of the SDF/QoS. Refer to 3GPP TS 29.212: Policy and Charging Control over Gx reference point, for more details.

Gxa: SM Support for Triggering APN AMBR Change

This scenario occurs when the PDN-specific AMBR is modified by the AAA and the PCRF has subscribed for the QOS_CHANGE Event Trigger. The HSGW shall send a CCR-Update with QoS-Information (UPDATE) for the PDN to update the AMBR information provided for the APN.

Sessmgr/IMSA support for sending CCR U with QoS Change for APN AMBR change is already present.

SM needs to call sessmgr_gxa_trigger at the appropriate place.

Gxa: Support for Enabling Rules/Rulebase in SM

HSGW supports enabling of pre-defined rules/rulebase from PCRF for Gxa interface. SM supports enabling the rules received from PCRF.

1. The pre-provisioned policy (policy-map, policy-group) needs to be configured in HSGW configuration. Based on the request in diameter messages (CCA, RAR) for inclusion or removal of a given policy-group/rulebase or policy-map/rulename, the rules are loaded and take effect for data tx/rx and QoS Check process.
2. The assumption here is that if HSGW receives a policy-group/rulebase name in diameter msg to load the rules, HSGW will be loading all of the policies within the given policy-group other than type template. If a policy is termed as type “template,” it will only be loaded if HSGW gets the rulename/policy-map in the diameter msg request.

   The case for deletion of the rules is similar.

3. Once the rules are loaded based on above request, it will be effective for rule matching for data transfer and QoS Check/TFT-matching process.

Gxa: Support for Sending Rule Report in Case of Loss of Bearer

Network Initiated QoS

If a bearer is terminated on the HSGW, the HSGW will generate a CCR-U with a charging rule report containing the list of rules affected by the event and a rule status of inactive.

Gxa: Support for Storing Packet Data ID

Each Packet-Filter-Information AVP shall include a packet filter identifier as provided by the PCRF in the QoS rule within the Packet-Filter-Identifier AVP identifying the previously requested packet filter being modified and, if the precedence value is changed, shall include packet filter precedence information within the Precedence AVP.

The Packet-Filter-Identifier AVP (AVP code 1060) is of type Octet String, and it indicates the identity of the packet filter. The packet filter identifier is assigned by the PCRF and within the scope of the PCRF is unique per UE.

Handling Hostnames Without the “topon/topoff” Label

Host names are expected to be configured with either “topon” or “topoff” as the first label in the DNS server. In absence of “topxx” label, host name should be treated as implicit “topoff” and first label of DNS returned host name should be stripped to yield the node name for use in topology match.

The same applies to P-GW FQDN supplied by AAA.

When P-GW host name does not have topxx label, APN and P-GW FQDN discovery are performed correctly by HSGW.

Node selection fallback is also done correctly.

HSGW Router Solicitation

CLI added to subscriber template to enable the time interval in milliseconds to wait for router solicit before sending the initial IPv6 router advertisement.

HSGW Support for APN-OI in S2a APN IE

If mag-service has “mobility-option-type custom2” configured, MAG will send APN-NI+OI in Service Selection field in PBU. APN-OI is constructed from IMSI in EAP NAI and will have the following format:

mnc<MNC>.mcc<MCC>.gprs

The HSGW will support P-GW lookup for initial attach using the APN. If the MIP6-Agent-Info header is not present, or empty, then the APN FQDN will be used, which has the format of:

<APN-NI>.apn.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org

Improved Dynamic P-GW Selection Mechanism by HSGW

During dynamic P-GW node selection by MME and HSGW, if the selected P-GW is unreachable, MME and HSGW select the next P-GW entry from the P-GW candidate list returned during the S-NAPTR procedure to set up the PDN connection.

Scenario

When eHRPD PDN comes up, PMIPv6 session is tried with first P-GW selected and if no reply is received for max-retransmission...

Previous Behavior

Reject the PDN.

New Behavior

If P-GW does not respond, HSGW tries with another P-GW if available based on DNS resolution results by starting with initial retransmission timeout as configured. There is no limit on the number of P-GW fallback attempts per PDN and HSGW will keep trying fallback as long as alternate P-GWs are available. The session may, however, get dropped if session-timeout gets triggered, in which case PMIPv6 PDN will also get deleted.

Lawful Intercept

The Cisco Lawful Intercept feature is supported on the HSGW. Lawful Intercept is a licensed enabled, standards-based feature that provides telecommunications service providers with a mechanism to assist law enforcement agencies in monitoring suspicious individuals for potential illegal activity. For additional information and documentation on the Lawful Intercept feature, contact your local Cisco sales representative.

Maximum Number of eHRPD PDNs Supported Per Session Configurable

Previous Behavior

Previously, the maximum number of eHRPD PDNs supported per subscriber session had a hard limit of three.

New Behavior

Now, the maximum number of eHRPD PDNs supported per session is configurable from 1 to 14. Default is 3.

Network Initiated QoS

The Network Initiated QoS control is a set of signaling procedures for managing bearers and controlling their QoS assigned by the network. This gives network operators full control over the QoS provided for its offered services for each of its subscriber groups.

If the UE supports Network Initiated QoS, then the UE shall include the MS Support of Network Requested Bearer Control indicator (BCM) parameter in the additional parameter list of the PCO option when sent in the vendor specific network control protocol (VSNCP) Configure-Request from the UE to the HSGW. Otherwise, the UE shall not include the MS Support of Network Requested Bearer Control indicator (BCM) parameter.

For Network Initiated QOS, three types of operations are permitted:

- Initiate flow request
- Deletion of packet filters for the specified traffic flow template (TFT)
- Modifications of packet filters for the specified TFT

Node Selection Error Case Handling, P-GW Support

Previously, PMIP P-GW was allowed to create a new session with handoff indication.

Now, when PMIP P-GW receives a PBU with Handoff Indicator set to 2 or 4 (indicating inter-tech handoff) and matching session for IMSI/APN is not found in either eHRPD or LTE, then PBU will be rejected with status code 159 BCE_PBU_PREFIX_SET_DO_NOT_MATCH.

Node Selection: P-GW IP Address Updated and Retrieved During Handover Description

If PGW-ID (either IP address or PGW-FQDN) is received in MIP6-Home-Agent-Info AVP on the STa interface, it is only used if one of the following conditions is met:

- PDN-GW-Allocation-Type AVP is absent
- PDN-GW-Allocation-Type is set to STATIC(0)
- PDN-GW-Allocation-Type is set to DYNAMIC and attach type is “Handover”

Otherwise, PGW-ID is ignored and P-GW is discovered by resolving the APN-FQDN.

Prefix-len in the IPv4 Home Address Request Option of the PBU Message

Previous Behavior

Prefix-len in the IPv4 Home Address Request Option of the PBU message sent to P-GW was 0x80.

New Behavior

Now, Prefix-len in the IPv4 Home Address Request Option of the PBU message sent to P-GW is 0x00.

Release 9 3GPP References Supported

The HSGW currently supports the following Release 9 3GPP specifications. Most 3GPP specifications are also used for 3GPP2 support.

- **3GPP TS 21.905**: Vocabulary for 3GPP Specifications
- **3GPP TS 23.401**: General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access

- **3GPP TS 23.402**. Architecture enhancements for non-3GPP accesses
- **3GPP TS 29.212**: Policy and Charging Control over Gx reference point
- **3GPP TS 29.214**: Policy and Charging control over Rx reference point
- **3GPP TS 29.229**: Cx and Dx interfaces based on Diameter protocol
- **3GPP TS 29.273**: 3GPP EPS AAA Interfaces

Support for Storing EPS_SUBSCRIBED_QOS_PROFILE Received from STa in sessmgr

If Default-Bearer-QoS is received over STa, the value is included in CCR-I. Any change of Default_Bearer_QoS via the Reauth procedure is included in the subsequent CCR-U.

Support for Stripping IMSI Prefix

TS 23.003, version 9.2.0, section 19.3.2 was updated as follows:

The NAI sent in the Mobile Node Identifier field in PMIPv6 will not include the digit prepended in front of the IMSI that is described above.

The current HSGW includes NAI received in EAP, and P-GW also expects this digit to be present. To support removing the leading digit, **`mobility-option-type-value standard`** configuration in MAG/LMA service will be used to support S2a MN-ID. There is no behavior change for **`custom1`** and it will continue to work as usual.

Added HSGW support for stripping IMSI prefix.

Completed P-GW changes to extract IMSI from NAI and handle cases when auth-mode digit is included or removed. **`mobility-option-type`** configuration is used and standard is expected to receive PBU without digit prepended.

In both HSGW/P-GW, PBU is expected to have <IMSI>@realm where IMSI field can only be maximum of 16 digits, including auth-mode. If it is more than 16 digits, then it is decoded as invalid IMSI format and IMSI will not be extracted.

In addition, **`mobility-option-type custom2`** configuration has been added for this feature. The standard will continue to work as before.

Termination-Cause AVP Missed in CCR-T Dictionary gxa-3gpp2-standard

Previous Behavior

The Termination-Cause was not sent in the Credit-Control-Request-Termination.

New Behavior

Now, the Termination-Cause AVP is sent in the CCR-T message.

UE Assigned Full IPv6 Address Reporting to AAA

S6b interface enhanced to pass the UE Assigned IP Address.

InTracer Features in Release 12.2

This section provides information on new InTracer features in release 12.2. For more information on InTracer, refer *InTracer Installation and Administration Guide*.

InTracer Query by MSISDN Support for 7600 Gateway

MSISDN support added to InTracer. User can search based by MSISDN.

InTracer Configuration support for 7600 SAMI platform

InTracer now supports configuration of 7600 for subscriber and equipment trace, which involves setting trace parameters like trace profile, transfer interval, buffer limit, access to NE, enabling/ disabling trace and viewing trace status and statistics.

InTracer scaling architecture

Architectural change is an enhancement of existing TCE application to support the high scalability and to support high load from gateway.

IPCF Features in Release 12.1

This section provides information on new IPCF features in Release 12.1.

Intelligent Policy Control Function (IPCF) provides policy control and charging rule functions in a core network.

IPCF acts as a PCRF functions supplemented with usage monitoring capability that enables policies around data consumption. IPCF interfaces with the PCEF over standard Gx interface for policy management and optionally over

Cisco IPCF is compliant in accordance with 3GPP standard in operator's core network. Some of the key functions of IPCF are to:

- Correlate service and charging information across PCEF and AF
- Derive and authorize the QoS information for the service data flow for session as well as bearer usage
- Ensure the PCEF user plane traffic treatment is in accordance with the user's subscription profile
- Provides network control regarding the service data flow detection and gating
- Select the appropriate charging criteria and mechanism apt for the data usage

For information about the IPCF solution, refer *Cisco ASR 5000 Series Intelligent Policy Control Function Administration Guide*

Diamproxy Capacity Improvement with one Gx Peer

Previous Behavior

Earlier, the Diameter proxy in master-slave mode used to load distribution to all the slave tasks based on peer-id of the incoming session. Thus all the sessions coming from the same peer will go to the same diamproxy.

This puts a binding on the client to use multiple peers if all the proxies have to be used.

New Behavior

In the new behavior, the sessions are distributed across different slaves/worker proxies based on a hash value calculated from the session-id. Thus, all the sessions having the same similar hash value will go to the same proxy.

This eliminates the need at client to have multiple peers to make use of all the proxies at PCRF.

IPCF Session Limit

Previous Behavior

Earlier, due to Gy flip on GGSN on GGSN-IPCF setup, GGSN would terminate its session without sending CCR-Termination message to IPCF. This created large number of sessions on IPCF. Some sessions were flushed through Inactivity-Timeout handling and Reauth-probe mechanism.

However, number of reauth probes were limited to 256 by congestion window at diameter peer on IPCF. As a result, Reauth-probe creation failed. In this case next cycle of probing will happen after 30 minutes. As a result, deletion of extra session was slowed down.

New Behavior

A timer based reauth-retry mechanism is added. If Reauth-probe creation fails, the PCC Sub session is inserted into a list under PCC-Policy service and a flag is set to indicate that reauth-retry will happen. Inactivity timer is stopped for the session. A free-running reauth-retry timer under the PCC-Policy service per Session Manager Instance with a timeout of 30 seconds will try to send reauth-probe for sessions present in the list. In every cycle, it will try up to 64 sessions. This number is derived as one fourth of default congestion window size for diameter peer (which is 256).

If retry of reauth-probe is successful, the session entry is removed from the list. On successful response for reauth-probe, inactivity timer is restarted. If reauth-probe response returns failure (UNKNOWN_SESSION_ID), session will be removed.

When reauth-retry timer under the PCC-Policy service finds that no session is present under PCC-Policy service, it is stopped. Once a session entry is added, it is restarted.

Impact on customer: In case of extra session creation of IPCF due to GGSN Gy flip, this mechanism of reauth-retry will allow IPCF to retransmit reauth-probe at a faster rate. As a result, once reauth probe response arrives from GGSN as UNKNOWN_SESSION_ID, these sessions will be cleared faster.

MCC/MNC based SSC Server Selection at IPCF

Previous Behavior

Earlier, IPCF had two mechanisms for SSC server selections: Round-Robin and Primary-Secondary. The selection happens at SPRMGR instance level. In case of Round-Robin, IPCF selects one SSC peer out of all configured in a Round-Robin fashion. In case of Primary-Secondary mechanism, IPCF configures to designate one peer as primary and another one as optionally secondary. IPCF sends all Sh requests to the primary peer. If primary server fails then IPCF sends Sh request to the secondary if it is configured and available.

Both Primary-Secondary and Round-Robin selection mechanism do not rely on any subscriber information.

New Behavior

The new behavior enables subscriber-based SSC peer selection, which makes use of subscriber details such as IMSI. According to ITU-T Recommendation E.212, IMSI is a subscriber identifier that consists of a three digit MCC (Mobile Country Code) and a 2/3 digit MNC (Mobile Network Code) as its prefix components. Subscribers are grouped according to their MCC-MNC values.

The SSC Peer Selection happens in SPRMGR (which is actually a AAMGR proclet). SPRMGR compares MCC, MNC and MSIN components present in Subscriber IMSI with the selection conditions configured and selects SSC peer when first condition match is found.

The feature is useful when IPCF is connected to multiple SSC severs and the subscriber database at SSC server is organized based on MCC-MNC components of subscriber IMSI. Operator can configure one or more (maximum 63) IMSI-based conditions under PCC-Sp-Endpoint. Each condition has a precedence value associated with it that decides the order of evaluation of conditions.

MNC values less than 10 not accepted by IPCF

Previous Behavior

It is observed that IPCF is not accepting MNC values which are less than 10 such as MNC values from 01 to 09. Currently, there are some operators which have MNC values between 01 and 09.

New Behavior

The new behavior enables the user to enter values from 01 to 09.

Peer Selection Statistics

Previous Behavior

Earlier, the statistics for all the precedence values (1 to 64) were displayed.

New Behavior

As per the new behavior, statistics for the configured precedence values are only displayed along with whether peer selection is success or failure.

SSC Peer Name Display in Statistics

Previous Behavior

Earlier, primary and secondary SSC peer names were not displayed when executing the command **show pcc-sp-endpoint statistics**.

New Behavior

As per the new behavior, primary and secondary peer names are displayed when executing the command **show pcc-sp-endpoint statistics**.

Protocol and Session Handling

Previous Behavior

IPCF sends RAR message as a periodic reauth-probe. If PCEF responds to this reauth-probe with RAA containing Result-Code set to any failure value, IPCF would terminate the PCC session.

New Behavior

IPCF shall terminate PCC Session only when PCEF responds to reauth-probe with RAR having Result-Code set to UNKNOWN_SESSION_ID (5002). For any other Result-code value session will not be terminated.

IP Services Gateway Features in Release 12.0

This section provides information on new IP Services Gateway (IPSG) features in Release 12.0. For more information on IPSG, refer the *IP Services Gateway Administration Guide*.

Volume Reporting over Gx

With this release, IPSG supports the Volume Reporting over Gx feature.

IP Services Gateway Features in Release 12.2

This section provides information on new IP Services Gateway (IPSG) features in Release 12.2. For more information on IPSG, refer the *IP Services Gateway Administration Guide*.

QoS Upgrade - Behavior Change

In earlier releases, in CCR-U message QoS-Upgrade AVP's value was always sent as QoS_UPGRADE_NOT_SUPPORTED.

This release onwards, with the support for QoS Upgrade, in CCR-I and CCR-U messages the QoS-Upgrade AVP's value is always sent as QoS_UPGRADE_SUPPORTED (only for IPSG).

LNS Features in Release 12.2

LNS Service Configuration Mode Commands

This section provides information on new LNS commands available in Release 12.2.

newcall

The following command configures new call related behavior

CLI (LNS Service Configuration Mode)

```
newcall duplicate-subscriber-requested-address { accept | reject }
default newcall duplicate-subscriber-requested-address
```

Mobility Management Entity Features in Release 12.0

This section provides information on new Mobility Management Entity (MME) features in Release 12.0.

3G/4G to 4G TAU Security Mode Reject Cause Code

When a Security mode reject happens for a mapped security context in case of 3G to 4G TAU, the cause code in TAU reject is now mapped to “Cannot Derive MS identity” (0x09). This change is specific to 3G/4G to 4G TAU and does not affect normal TAU.

Previous Behavior

Security mode reject triggered TAU reject with the cause code “Illegal ME”.

New Behavior

Security mode reject triggers TAU reject with the cause code “Cannot derive MS identity”.

Default Heuristic Paging - Behavior Change

Previous Behavior

If heuristics paging is turned on for the mme-service, the following heuristics paging behavior is used:

"1. Page the last eNodeB from which the UE contacted the MME in the last TAI from which the UE contacted the MME.

"2. Page all eNodeBs in the last TAI from which the UE contacted the MME.

"3. Page all eNodeBs in all TAIs present in the TAI list assigned to the UE.

When heuristic paging is enabled, the MME tracks the last TAI from which the UE contacted the MME and the last eNodeB from which the UE contacted the MME.

Paging to the last eNodeB and the TAI from which UE was last heard is done only once. max-paging-attempts configured in the mme-service is used only for TAI list paging.

New Behavior

For paging requests for Circuit Switch (CS) calls, the MME no longer follows this staged paging behavior. Instead, it follows the standards-defined paging mechanism of paging all eNodeBs in all TAIs present in the TAI list assigned to the UE (all-enb-all-tai). Only one attempt is made with no retries.

Combined TA/LA Update - Behavior Change

In cases where a “Combined TA/LA Update” does not result in a LOCATION_UDATE_REQ towards the MSC/VLR, the MME now sends a “Combined TA/LA Update” in the EPS Update which results in TAU Accept.

PDN Disconnect Procedure - Behavior Change

If the MME is processing a service request, and the MME receives a PDN DISCONNECT REQUEST, the MME will start a MME Initiated PDN DISCONNECT procedure once the Service Request processing is done.

3G to 4G TAU Request with Erroneous EPS Bearer Context Status

Previous Behavior

When the MME received a 3G to 4G TAU request with the EPS Bearer Context status with the value zero (no active bearers), it would examine the EPS Bearer Context Status only after performing a Context status transfer with the old SGSN.

New Behavior

The MME now will reject the TAU request immediately, instead of rejecting the request after performing a Context Request transaction with the old SGSN. This new behavior optimizes the Gn/Gp/S3 TAU cell reselection call flow. The old SGSN will no longer receive an SGSN Context request from the MME when there are no active 3G PDP Contexts.

TAU-based Gn/Gp Handover from 3G SGSN to MME - Behavior Change

Cell re-selection from a 3G SGSN to an MME based on receiving an S1AP Init UE-based TAU request is now supported.

Handover Support for Release 8 SGSNs

The S3 interface facilitates user mobility between an MME and a Release 8 SGSN providing for the transfer of the UE context between the MME and the SGSN.

Circuit Switched Fall Back - Voice Support Over SGs

Circuit Switched Fall Back enables a UE to camp on an E-UTRAN cell and originate or terminate voice calls through a forced switchover to the CS domain.

Equipment Identity Register (EIR) S13 Timeout and Failure Handling

The MME now supports timeout and failure handling for the EIR on the S13 interface. Configuration of the timeout and/or failure response is now available. Refer to the **`attach`** and **`tau`** commands in the "Mobility Management Entity Command - Modified in Release 12.0" in the *Configuration Management* chapter for more information.

IKEv2 IP Security Support on S1-MME

IP Security (IPSec) on the S1-MME interface is a node-to-node IKEv2 tunnel that can be configured to assume the characteristics of either a pre-configured tunnel or a dynamic tunnel.

Pre-configured node tunnels are fully qualified IPSec tunnels. Each IPSec tunnel is configured with parameters including pre-shared key, local and remote IP addresses, crypto hashes, groups, algorithms and the access control list (ACL).

Node-to-node dynamic tunnels are generated dynamically as the connections are initiated by different nodes in the LTE network. Each IPSec tunnel does not need to be pre-configured for each required parameter, instead it uses a common template for some parameters, like crypto algorithms, hashes, and groups. Other parameters are fetched dynamically from the tunnel requests like IP addresses and traffic selectors. Authentication information is fetched dynamically via certificates.

Typically, the eNodeB initiates an IPSec tunnel to the MME. The MME service is responsible to verify the configuration and use an IPSec API to make the MME listen on the service address for IKE requests.

The S1-MME Interface carries SCTP signaling traffic that flows through an IPSec tunnel if it is configured. When a UE needs to connect to the Internet, it initiates a connection to an eNodeB which then tunnels its traffic to an MME using an SCTP connection. Any further UEs using the same eNodeB to communicate to the same MME will subsequently use the same SCTP and hence the same IPSec Tunnel according to the LTE standard.

X.509 Certificate-based Peer Authentication

The MME supports X.509 certificate-based peer authentication for IPSec tunnels over the S1-MME interface.

S6a Multi-Homing

The MME service supports up to four SCTP bind end point IPv4 or IPv6 addresses for the S6a interface.

PSC3 Hardware Support

The MME service supports the use of the Packet Service Card 3 in this release.

Dynamic Discovery of HSS Realm

The MME now supports behavior that allows the peer realm of the HSS to be determined by the MCC and MNC in the subscriber's IMSI. Prior behavior was that the HSS must be statically configured in the MME.

Error Message Correction for Maximum Peer SGSN RNC/RAI Configurations

The MME now correctly identifies error conditions related to reaching the maximum number of configured peer SGSN RNCs and RAIs.

Previous Behavior

When the maximum number of peer-SGSN RAI entries were exceeded (32), the error message displayed was: **Failure: Unable to retrieve information: error 390:0**

When the maximum number of peer-SGSN RNC-ID entries were exceeded (32), the error message displayed was: **Failure: Unable to retrieve information: error 390:0**

New Behavior

When the maximum number of peer-SGSN RAI entries are exceeded (32), the new error message displayed is: **Failure: Maximum number of Peer SGSN RAI entries already configured**

When the maximum number of peer-SGSN RNC-ID entries are exceeded (32), the new error message displayed is: **Failure: Maximum number of Peer SGSN RNC-ID entries already configured**

NAS/S1AP Message Re-Order and Piggybacking

Previous Behavior

NAS messages received in an incorrect order were piggybacked without re-ordering and retried causing error conditions.

New Behavior

If NAS messages require re-ordering, piggybacking is not performed. For example, for a piggybacked Create Bearer Request, if there is a re-order of the NAS/S1AP message, then the Create Bearer Response message will not be piggybacked with the Modify Bearer Request message.

NRI Length Configuration

The MME now has the ability to configure the network resource identifier (NRI) length used for source SGSN discovery via NRI-FQDN based DNS resolution. MME now uses the NRI field to resolve peer SGSN during TAU handoffs and Attaches with mapped GUTI. The length of the NRI field can now be configured for a given PLMN. This allows the MME to extract NRI unambiguously from P-TMSI. For more information, refer to the **`nri`** command in the *Mobility Management Entity Commands - New in Release 12.2* section of the *Configuration Management* chapter of this change reference.

Previous Behavior

The MME only supported RAI-based FQDNs to resolve source SGSNs.

New Behavior

The MME now also supports using NRI-based FQDN to resolve the source SGSN. More specific DNS entries can be configured corresponding to each SGSN. SGSNs are now not required to support relay functionality in order for SGSN Context Request and Identification Request messages to reach source SGSN.

This change was first introduced in version 12.2, and has since been added to version 12.0.

Mobility Management Entity Features in Release 12.2

This section provides information on new Mobility Management Entity (MME) features in Release 12.2.

Increased SGS Interface Configuration Limits

The limits for various operational capacities have been increased in this release as described in the following table.

Table 1-3 Operational Limits

	Previous Limits (12.2)	New Limits
Maximum Number of VLRs	32	48
Maximum Number of Pools + Non Pool Areas (combined total)	8	48
Maximum Number of LACs per Pool/Non Pool Area	16	96
Maximum Number of Hash lists per pool area	32	48
Maximum Number of TAC to LAC Mapping Lists	32	64
Maximum Number of mapping per TAC to LAC List	8	8

PDN Disconnect Procedure - Behavior Change

If the MME is processing a service request, and the MME receives a PDN DISCONNECT REQUEST, the MME will start a MME Initiated PDN DISCONNECT procedure once the Service Request processing is done.

Attach/TAU Attach Reject Behavior Change

Previous Behavior

For ATTACH/TAU procedures, if the ATTACH REQUEST passes integrity checks, but an IMSI mismatch with SGSN occurs, the MME rejects the call with cause code #3: Illegal UE.

New Behavior

For ATTACH procedures, if the ATTACH REQUEST passes integrity checks, but an IMSI mismatch with SGSN occurs, then MME assumes that MME mapping is correct and proceeds with authentication with that IMSI.

For TAU ATTACH procedures, the cause code for reject has been changed to #9: UE identity cannot be derived by the network.

Enhanced EMM Cause Code Mapping Control

Previously the MME supported configuration of NAS cause codes to signal to the UE when the MME receives a Diameter result code of 5421 (RAT not allowed) from the HSS. The following EMM cause codes were previously supported for this use:

"#15 "No suitable cells in tracking area", or

"#13 "Roaming not allowed in this tracking area", or

"#12 "Tracking area not allowed"

In this release, the following additional diameter result codes are now also supported. The following table also lists the default EMM cause codes to which each diameter result code is mapped by default. These mappings can be altered using the following CLI command:

Table 1-4 Diameter Result Codes

Diameter Result Code	Default Cause Code Signaled to the UE
DIAMETER_ERROR_USER_UNKNOWN (5001) (experimental result code) DIAMETER_ERROR_USER_UNKNOWN (5030)	#8 "EPS services and non-EPS services not allowed"
DIAMETER_ERROR_UNKNOWN_EPS_ SUBSCRIPTION (5420)	#15 "No suitable cells in tracking area"
DIAMETER_ERROR_ROAMING_NOT_ALLOWED (5004)	#11 "PLMN not allowed"
DIAMETER_AUTHORIZATION_REJECTED (5003)	#15 "No suitable cells in tracking area"
DIAMETER_UNABLE_TO_COMPLY (5012)	#17 "Network failure"
DIAMETER_INVALID_AVP_VALUE (5004)	#17 "Network failure"
DIAMETER_UNSUPPORTED_FEATURE (5011)	#15 "No suitable cells in tracking area"
Any code that is not specified above	#17 "Network failure".

Refer to the **`diameter-result-code-mapping`** command in the *Mobility Management Entity Command - Modified in Release 12.2* section in the *Configuration Management* chapter for more information.

Configurable Target RNC-ID to Target eNodeB-ID Mapping for Inter-RAT Handovers

The MME now provides the ability to configure how the fields in the Target RNC-ID are mapped to the Target eNodeB fields during a UMTS to E-UTRAN relocation.

Refer to the **`policy inter-rat`** command in the *Mobility Management Entity Command - Modified in Release 12.2* section in the *Configuration Management* chapter for more information.

Show APN Profile Command Output

The **`show apn-profile full name`** command now correctly displays the P-GW information configured for the specified APN Profile.

4G to 3G TAU Failure - Behavioral Change

The MME now rejects 4G to 3G TAUs when a Context response with “Uplink TEID Control Plane: 0x00000000” is received.

Note: Uplink TEID Control Plane: 0x00000000 denotes that the PDP context created in 3G is using GTPv0 but Gn interface supports GTPv1. Therefore, the MME must reject such relocations. In this case, the UE must make a new attach to a 4G MME.

Previous Behavior

During 3G to 4G Gn/Gp TAU, when the SGSN sent a Context response with “Uplink TEID Control Plane: 0x00000000”, the MME would to proceed with TAU procedure and send a Context_Ack followed by Create_session_request to the S-GW/P-GW. When the P-GW/S-GW rejected with the cause EGTP_CAUSE_CONDITIONAL_IE_MISSING (0x67) in create session, this meant that the MME sent PGW-CONTROL-TEID as 0x00000000 in Create_session_request. Therefore, the P-GW/S-GW rejected it and the MME sent TAU_Reject to UE.

New Behavior

When the MME receives a Context_response with “Uplink TEID Control Plane: 0x00000000” from the SGSN, the MME rejects the TAU procedure with following messages:

Context_Ack with Cause: 0xCB (GTP_OPTIONAL_IE_INCORRECT) right away without sending Create_session_request to SGW/PGW

TAU_REJECT with cause NO EPS BEARER CONTEXT ACTIVATED (0x28)

MME Error Code Changes

Various mme-app error codes were reported as Log Level: **error** (event-id 147000) incorrectly, and have been downgraded to Level: **unusual** (event-id 147002) or **info** (event-id 147003).

S1-HO Based Location Reporting- Behavioral Change

Previous Behavior

The MME was sending the RequestType IE to target eNodeB in S1AP Location report control message.

New Behavior

The MME now sends the RequestType IE to target eNodeB in S1AP request message.

3G to 4G TAU Request with Erroneous EPS Bearer Context Status - Behavioral Change

Previous Behavior

When the MME received a 3G to 4G TAU request with the EPS Bearer Context status with the value zero (no active bearers), it would examine the EPS Bearer Context Status only after performing a Context status transfer with the old SGSN.

New Behavior

The MME now will reject the TAU request immediately, instead of rejecting the request after performing a Context Request transaction with the old SGSN. This new behavior optimizes the Gn/Gp/S3 TAU cell reselection call flow. The old SGSN will no longer receive an SGSN Context request from the MME when there are no active 3G PDP Contexts.

Support for Additional VLRs

Previous Behavior

The MME supported a maximum of 16 VLRs per SGs service.

New Behavior

The MME now supports the creation of up to 32 VLRs per SGs service.

VLR Offload

The MME now supports a maintenance command enabling an operator to enable or disable 'offload' mode for a specified VLR. This capability enables operators to preemptively move

subscribers away from an SGs interface associated with an MSS which is planned for maintenance mode.

When this offload command is set on the MME, all sessions matching this VLR are marked with an ‘offload’ flag. During the next Combined/Periodic TAU, the MME performs a mandatory Location update towards MSC.

The VLR offload functionality and MME offload functionality can be used in a mutually exclusive fashion, such that activation of one prevents activation of the other (and vice versa).

Refer to the **`sgs offload sgs-service`** command in the *Mobility Management Entity Command - New in Release 12.2* section in the *Configuration Management* chapter for more information.

Modify Bearer Request - Behavioral Change

Previous Behavior

Modify Bearer Requests always included the APN-Aggregate Maximum Bit Rate (AMBR) information element.

New Behavior

The APN-AMBR IE is now only included for PS handovers.

DNS Lookup for Periodic TAU - Behavioral Change

Previous Behavior

SGW relocation occurred irrespective of TAU update type.

New Behavior

SGW selection and relocation does not occur if the TAU update type is 'PERIODIC UPDATING'.

Default Bearer Context Activation - Behavioral Change

Previous Behavior

During a Default Bearer Context activation procedure, the MME sent an ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST message but did not include the operator identifier (`mnc <mnc>.mcc<mcc>.gprs`) in the Access Point Name information element.

New Behavior

The APN information element now includes both the operator identifier and network identifier in ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST messages.

Network Sharing Support

To support a network sharing configuration where core network elements (MME, SGW, PGW) are shared between different service providers, the MME service can now be configured with multiple local PLMNs per service. Each mme-service is now able to process multiple PLMNs and indicate this to the eNodeb during S1 SETUP procedures.

The configuration of these additional PLMNs is implemented using the **`network-sharing`** command within the mme-service config mode.

Refer to the *MME Commands - New in Release 12.2* section in the *Configuration Management* chapter of this guide and to the *Cisco ASR 5000 Series Command Line Interface Reference* for details of this new CLI command.

2G to 4G Gn/Gp SGSN to MME TAU Requests - Behavioral Change

Previous Behavior

During a 2G to 4G Tracking Area Update (TAU), the MME sent the SGSN a Context Request message. If the SGSN replies with an SGSN Context Response which includes no PDP contexts, the MME then sent back a Context Acknowledge message with a GTP_MANDATORY_IE_MISSING error, and the TAU would fail.

In this case, the MME assumed that the UE would never perform a TAU Attach with zero PDP Contexts active in 3G. As a result, the SGSN Context Response with missing PDP contexts was treated as an error condition.

New Behavior

If the SGSN Context Response is received with no PDP contexts, the MME now responds with an SGSN Context Acknowledge with cause 'Request Accepted' allowing the Gn/Gp context transfer, but then rejects the TAU with cause 'No EPS bearer context activated'.

Remove Preamble from Target-ID of Relocation Request - Behavioral Change

Previous Behavior

The MME included the preamble in the target-id of relocation requests (sender side) and always expected the preamble in the target-id of relocation request (receiver side).

New Behavior

By default (on sender side), the MME no longer includes the preamble in the target-id of relocation requests. On receiver side, the SGSN/MME will act per target-id length. If the target-id length is 8, then the SGSN/MME will act as target-id without preamble.

To enable the previous behavior, refer to the **`gtpc`** command in the Mobility Management Entity Commands - Modified in Release 12.2 section of the Configuration Management chapter of this change reference.

NRI Length Configuration

The MME now has the ability to configure the network resource identifier (NRI) length used for source SGSN discovery via NRI-FQDN based DNS resolution. MME now uses the NRI field to resolve peer SGSN during TAU handoffs and Attaches with mapped GUTI. The length of the NRI field can now be configured for a given PLMN. This allows the MME to extract NRI unambiguously from P-TMSI. For more information, refer to the **`nri`** command in the Mobility Management Entity Commands - New in Release 12.2 section of the Configuration Management chapter of this change reference.

Previous Behavior

The MME only supported RAI-based FQDNs to resolve source SGSNs.

New Behavior

The MME now also supports using NRI-based FQDN to resolve the source SGSN. More specific DNS entries can be configured corresponding to each SGSN. SGSNs are now not required to support relay functionality in order for SGSN Context Request and Identification Request messages to reach source SGSN.

Regional Zone Code Restriction

Regional Zone Code Restriction allows an operator to control the areas in which a UE can roam in to receive service. The code representing the zone in which a UE is to be offered service by the network can be configured in the HSS or using local provisioning in the MME.

Release 9 3GPP References Supported

The MME currently supports the following Release 9 3GPP specifications:

- 3GPP TS 24.301 V9.5.0 (2010-12): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3 (Release 9)
- 3GPP TS 29.274 V9.5.0 (2010-12): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3 (Release 9)
- 3GPP TS 29.272 V9.5.0 (2010-12): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; 3GPP Evolved Packet System (EPS); Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol (Release 9)
- 3GPP TS 36.413 V9.5.0 (2010-12): 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access Network (E-UTRAN); S1 Application Protocol (S1AP) (Release 9)

Circuit-Switched Fallback

Support for PS Suspension/Resumption Message - Behavioral Change

The MME now supports the suspend notification on the S3 interface from the SGSN per 3GPP TS 23.272 (9.5.0) and TS 29.274 (9.4.0). The suspend notification is received and responded to by the eGTP-C demux process.

SGs SCTP Multi-homing Support

The SGs interface between the MME and the MSC/VLR now supports SCTP multi-homing. Refer to the **`bind`** and **`vlr`** commands in the “Mobility Management Entity Commands - Modified in Release 12.2” section of the Configuration Management chapter for more information.

SGs Service Distribution

The MME Demux task now learns about SGs services, and configured VLRs, and assigns them to MME Managers based upon a hash algorithm.

Emergency Cause Code Support

CSFB mobile emergency calls now use the emergency cause code to indicate to the eNodeB that the call is for emergency purposes. The CS-Fallback-High-Priority cause code is supported in Release 9.

IMSI Paging

Per section 5.1.3.1 of 3GPP TS 29.118, the MME now supports IMSI paging based on the following from the specification:

If the UE is not known and the “MME-Reset” restoration indicator at the MME is set to “true”, the MME shall handle the paging request as follows:

- if the MME only supports “SMS only”, the MME shall return an SGsAP-PAGING-REJECT message to the VLR indicating in the SGs cause information element “Mobile terminating CS fallback call rejected by the user”;
- if the SGsAP-PAGING-REQUEST message includes the Location area identifier information element, the MME shall page the UE in all the tracking areas served by the MME that can be mapped to the location area indicated in the Location area identifier information element; or
- if the SGsAP-PAGING-REQUEST message does not include the Location area identifier information element, the MME may page in all the tracking areas served by the MME, or the tracking areas served by the MME and by the VLR.

NOTE: The MME can initiate the paging procedure using IMSI with CN domain indicator set to “PS” to request the UE to initiate the attach procedure as described in 3GPP TS 24.301.

Dual Addressing PDP Contexts

Support for Dual Addressing on Pre-release 8 SGSNs (Gn/Gp) - Behavioral Change

The MME now supports dual-addressing for all network nodes including pre-release 8 SGSNs over Gn/Gp.

Dual Addressing PDP Contexts

Support for Dual Addressing on Pre-release 8 SGSNs (Gn/Gp) - Behavioral Change

The MME now supports dual-addressing for all network nodes including pre-release 8 SGSNs over Gn/Gp.

Equipment Identity Register (EIR) S13 Timeout and Failure Handling

The MME now supports timeout and failure handling for the EIR on the S13 interface. Configuration of the timeout and/or failure response is now available. Refer to the **`attach`** and **`tau`** commands in the "Mobility Management Entity Command - Modified in Release 12.2" in the *Configuration Management* chapter for more information.

Radio Information Management (RIM) Behavioral Change

The MME supports RAN Information Management (RIM) procedures as defined in 3GPP TS 23.401 on the S1-MME, S3, Gn, and S10 interfaces.

S1-MME Enhancements

S1AP Cause and RANAP Cause Code Mapping - Behavioral Change

S1AP and RANAP cause codes are mapped as directed in 3GPP TS 23.401 (V9.7.0) and TS 29.010 (V9.2.0).

MME Support for (RIM) Information Exchange Between eNodeB and RNC - Behavioral Change

The MME now supports the transparent exchange of RIM information that helps target an RNC to establish RRC connection with the UE.

Support for eNB/MME (S1-MME) Direct Information Transfer Procedure - Behavioral Change

The eNB/MME Direct Information Transfer procedure transfers RAN information between an eNB and an MME in unacknowledged mode. The MME does not interpret the transferred RAN information. This procedure uses non-UE associated signalling.

Support for eNB/MME Configuration Transfer - Inter-MME - Behavioral Change

The eNB/MME Configuration Transfer procedure transfers RAN configuration information between the eNB and the MME in unacknowledged mode. The MME does not interpret the transferred RAN configuration information.

Support for IPv6 IPSec and Multi-homing over S1-MME

The S1-MME interface now supports IPv6 IPSec including multi-homing.

SON Information Transfer Over S1-MME - Behavioral Change

The MME now supports SON information transfer via MME/eNB Configuration Transfer messages defined in 3GPP TS 36.413.

S1-MME Initiated IPSec Tunnel - Behavioral Change

The MME now supports the initiation of IPSec tunnels to the eNodeB if the following conditions exist:

- The first tunnel setup is always triggered by eNodeB. This is the tunnel over which initial SCTP exchanges occur.
- MME initiates additional tunnels to the eNodeB after SCTP connection is setup if
  - the MME is multi-homed: a tunnel is initiated from MME's second address to eNodeB.
  - the eNodeB is multi-homed: Tunnels are initiated from MME's primary address to each secondary address of eNodeB.
  - both of the above: A tunnel is initiated from each of MME's addresses to each address of eNodeB.

  In all three cases, the MME does not initiate a duplicate tunnel between the same end points if such a tunnel already exists, either because the eNodeB initiated them previously or because the tunnels from a previous initiation by the MME were not torn down.

If there is collision, for example, if the eNodeB also initiates a tunnel in the meantime, the tunnel initiated by eNodeB is given preference and the MME-initiated tunnel is torn down. This can happen both after an MME-initiated tunnel has been established or is waiting establishment.

Tunnels initiated by the MME are not torn down when the SCTP associations on the tunnels no longer exist.

IPv6 Interface Support - Behavioral Changes

S3/S10/S11 IPv6 behavioral Changes

The changes include MME selecting an IPv6 address for a peer-node in S11/S10/S3 interface.

There is no change in functional behavior over the S11/S10/S3 interfaces.

IP versions over S11/S10/S3 are not dependant on each other. For example, the MME may use IPv6 over S11 and IPv4 over S10 (provided the MME-EGTPC-Service is bound to both IPv6 and IPv4 address).

The logic for selecting an S-GW/peer-MME/peer-SGSN is now: preference is given for IPv6 addresses. IPv4 addresses are ignored if IPv6 addresses are present. This applies to

weighted selections using the TAI database, as well. Weights for IPv4 addresses are ignored if IPv6 addresses are present (only IPv6 addresses are load-balanced if present).

If the MME-EGTPC-Service is bound to an IPv4 address and there are only IPv6 addresses available during peer node selection (and vice versa), it is considered as a node selection failure (reason: No suitable addresses available).

Lawful Intercept

TCP Proxy Support

TCP Proxy support is now available for Lawful Intercept on the MME. Contact your local sales representative for detailed information.

Notification of LI Target Provision Modification/Deletion

The MME now supports the ability to send notifications to LI administrators when an existing LI target provision has been modified or deleted. CP Proxy support is now available for Lawful Intercept on the MME. Contact your local sales representative for detailed information.

S3 Interface Enhancements

IPv6 Support

The S3 interface now supports IPv6 addressing.

MME to 2G SGSN (GERAN) RAU Attach Support - Behavioral Change

The MME now supports RAU-based attach procedures to a 2G SGSN over the S3 interface as defined in 3GPP TS 23.401.

2G SGSN (GERAN) to MME TAU Attach Support - Behavioral Change

The MME now supports TAU-based attach procedures from a 2G SGSN over the S3 interface.

S10 Interface IPv6 Support

The S10 interface now supports IPv6 addressing.

S11 Interface Enhancements

IPv6 Support

The S11 interface now supports IPv6 addressing.

NAS Protocol Enhancements

Additional PDN Connectivity - Behavioral Change

This feature applies to additional PDN connection for an APN that already has an existing PDN connection, all within a UE context. In such situations, the additional PDN connection uses the same P-GW as the existing connection if both the following conditions are met:

- New connection uses dynamic discovery to obtain P-GW address.
- PGW for the existing connection was discovered dynamically.

Dynamic discovery refers to APN FQDN based DNS resolution.

DNS discovery will still happen for the new PDN request as the fallback list is built up front using the existing design. This avoids changes to NAS FSM. But the requests will be fed from local cache and external requests will be rare unless the TTL is very low.

The following INFO level mme-app log is added to indicate the re-use.

```
2011-Feb-22+16:10:02.742 [mme-app 147003 info] [1/0/21528 <sessmgr:1>
mme_app_util.c:10826] [callid 00004e29] [context: ingress, contextID: 2]
[software internal system syslog] Existing PGW for same APN re-used.
```

NOT SUPPORTED:

The P-GW re-use does not apply if the P-GW for the existing connection was allocated statically by any of the following means:

- Static Pool
- Static allocation by HSS (by IP address or by P-GW FQDN)
- Fallback to Static Pool because of DNS discovery failure

Support for Out-of-order Reception of Default and Dedicated Bearer UE Responses - Behavioral Change

The MME now does not retry the dedicated bearer request even if the dedicated bearer response is received before the default bearer response, once a successful default bearer response is received.

Non-delivered NAS Message Handling - Behavioral Change

The NAS message non-delivery handling is based on the following logic:

If the message could not be delivered due to an intra-MME handover and the target TA is included in the TAI list, then upon successful completion of the intra-MME handover the MME retransmits the message. If a failure of the handover procedure is reported by the lower layer and the S1 signalling connection exists, the MME retransmits the message.

NAS Messages Affected:

- EMM messages
  - GUTI Reallocation Command - Not supported since it is not implemented yet
  - Authentication Request - Supported, request resumed after HO
  - Security Mode Command - Supported, request resumed after HO
  - Identity Request - Not relevant to handover
  - EMM Information - Not supported
  - Detach Accept - Not supported

  - Detach Request - A handover is rejected if a detach request is pending, hence not relevant
  - TAU Accept - Not supported
  - Notification Procedure (srvcc) - Not supported
- ESM messages
  - Activate Default Bearer Request - Supported, request resumed after HO
  - Activate Dedicated Bearer Request - Supported, request resumed after HO
  - Deactivate Bearer Request - Supported, but not resumed after HO, since during HO the relevant PDN or bearer is deleted
  - ESM Information Request - Not supported
  - Modify EPS Bearer Request - Supported, request resumed after HO
  - ESM Status - Not supported

Monitor protocol supports decoding of S1AP NAS Non-delivery indication message. The NAS protocol selector shall not show these message since these are not messages sent by UE.

S1AP statistics count the NAS Non-delivery indication message. The un-delivered messages are not counted against NAS statistics.

UMTS to LTE ID Mapping

UMTS networks are configured with LACs allocated from the reserved space of 32K to 64K. In LTE networks, this space is typically reserved for MME group IDs. To overcome this issue during inter-RAT handovers, the MME can now be configured with mappings between LACs and MME group IDs.

Single Radio Voice Call Continuity

Voice over IP (VoIP) subscribers anchored in the IP Multimedia Subsystem (IMS) network can move out of an LTE coverage area and continue the call over the circuit-switched (CS) network through the use of the Single Radio Voice Call Continuity (SRVCC) feature. The smooth handover of the VoIP call does not require dual-mode radio.

To support SRVCC functionality on the MME, an Sv reference point is included providing an interface to the enhanced Mobile Switching Center (eMSC) server responsible for communicating with the MME during the handover process.

Emergency Sessions

The MME supports the creation of emergency bearer services which, in turn, support IMS emergency sessions. Emergency bearer services are provided to normally attached UEs and to UEs that are in a limited service state (depending on local service regulations, policies, and restrictions).

APN AVPs

Wild-card Selected APN Information Now in APN AVPs - Behavioral Change

When APN selection is based on wild-carded APN-Information, the Update-Location-Request of S6a interface will now contain the Active-APN list along with Specific-APN-Info under the list. Below is the new definition of both the AVPs:

Active-APN ::= <AVP-Header: 1612 10415 Type:GROUPED Flags: M >

{ Context-Identifier }
{ Service-Selection }
{ MIP6-Agent-Info }
{ Visited-Network-Identifier }
*[Specific-APN-Info]
*[AVP]

Specific-APN-Info ::= <AVP-Header: 1472 10415 Type:GROUPED Flags:M >

{ Service-Selection }
{ MIP6-Agent-Info }
[Visited-Network-Identifier]
*[AVP]

Previous Behavior:

- Service-Selection and MIP6-Agent-Info AVPs were NOT present under Active-APN level if Specific-APN-Info is present.
- Visited-Network-Identifier AVP was NOT present under Specific-APN-Info level.

New Behavior:

Service-Selection, MIP6-Agent-Info and Visited-Network-Identifier AVPs will be present under both Active-APN as well as Specific-APN-Info AVP.

MUR Features in Release 12.0

This section provides information on new Mobility Unified Reporting (MUR) features in Release 12.0.

DSL Reports

The current release of MUR provides the following details for DSL reports:

- Traffic analysis — uplink DSL, downlink DSL and total DSL traffic including daily weekly, and monthly aggregation/distribution.
- DSL traffic categorization — total P2P traffic over DSL, IP traffic, web traffic, etc.

- Top N% DSL subscribers.
- Comparison of total DSL traffic versus total UMTS traffic.

IMPORTANT

The DSL reports can be generated only when DSL is configured as an APN group during MUR software installation/upgrade.

Except the TopN% DSL subscribers, all other DSL reports can be viewed under the **DPI** tab by selecting appropriate dimensional filters.

IMPORTANT

The discrimination between DSL and UMTS traffic will be based on the APN Name attribute in the EDR file.

Enabling PUSH model for MUR Reporting

In the earlier releases, L-ESS was used to pull the EDRs from the chassis for reporting purpose.

Release 12.0 onwards, for all new deployments of MUR that use either Sun Netra X4270 or UCS C460 M2 server and run Red Hat Linux, L-ESS is NOT required as the ASR 5K EDR module can be configured to push the xDRs directly to the MUR reporting server. Push from ASR 5K is the Cisco recommended deployment model. Currently, L-ESS is supported only on Solaris platforms. Existing deployments where L-ESS is installed, to pull EDRs from ASR 5K, may continue with their deployment model in the 12.0 version of MUR Software Release and later.

Exporting Reports in CSV Format

MUR has the capability of exporting reports in Comma Separated Value (CSV) format in addition to PDF and Excel formats. This can be accomplished through the GUI by clicking the csv icon available in the tabular representation of all the reports in the **HOME** and **DPI** tabs.

Extended Support for Multiple BS Counter/Index Selections

In this release, MUR no longer supports the limitation of selecting only 15 bulkstats counters/indices at a time. Now, there is no defined limit as such; users are allowed to select any number of counters and indices simultaneously.

Charts will not be displayed if more than 15 indexes or 4 counters are selected. However, the data will be displayed in the **Table** tab of the BS/KPI reporting page.

HTTP User Agent Reports

MUR generates HTTP User Agent (UA) reports and/or UA group reports that are primarily used for ASR 5000 based Modem tethering detection.

In this release, MUR supports the following reports:

- Daily/weekly/monthly TopN User Agent Group report
- Daily/weekly/monthly TopN individual User Agent Group report - per APN
- Daily/weekly/monthly TopN individual User Agent Group report - per TAC
- Daily/weekly/monthly TopN individual User Agent report
- Daily/weekly/monthly TopN individual User Agent report - per APN
- Daily/weekly/monthly TopN individual User Agent report - per TAC

The MUR solution also provides a utility to export Top N User-Agent list to a text file based on the given level of tethered traffic. This text file contains pre-formatted CLI file with the configured ruledefs and group-of-ruledefs that need to be applied to the ASR 5K system.

IMPORTANT

Currently, MUR does not support UA report generation for historical data as the data tables does not contain User Agent, APN, and TAC. Also, note that any changes made to the APN/TAC/UA group configurations will not be applied to the old data.

Modifying Mandatory EDR Settings

The reporting EDR file contains multiple attribute fields like *sn-start-time* and *sn-end-time*; some of them are considered mandatory depending on the gateway and reporting types.

Currently, MUR mandates *sn-start-time* and *sn-end-time* fields in the flow EDR. If the EDR contains the fields *sn-flow-start-time* and *sn-flow-end-time* then MUR will pick values from these fields. However, the *sn-flow-start-time* and *sn-flow-end-time* fields are not mandatory.

In a particular deployment, if the EDR receives only *sn-flow-start-time* and *sn-flow-end-time* fields, then the mandatory settings for *sn-start-time* and *sn-end-time* should be disabled through the **System** menu on the GUI.

MUR User Administrative Limitations

In the current release, the following limitations were imposed with respect to user permissions and privileges:

- All MUR administrators have access to **USERS** and **GROUPS** menu in the **Admin** tab available on the MUR GUI.
- Administrator with *admin* user name will have the rights to modify and delete all the MUR users' accounts. Only users with *admin* user name can modify its own password. Only admin user will be able to delete any administrator or operator user accounts.

- Administrator other than users with *admin* user name will have rights to delete the MUR users except admin user and modify user accounts except their passwords.
- After modifying user role from Administrator to Operator and vice-versa, the user should alter the configuration on the GUI to lock/unlock the user account accordingly.

MUR with Support for UCS/RHEL 5.5

In this release, a custom Red Hat Enterprise Linux OS (Cisco MITG RHEL v5.5) has been introduced to support MUR running on the Cisco UCS platforms.

Release 12.0 onwards, for MUR it is recommended to use UCS C460 M2 server running MITG Customized RHEL 5.5. For information on the complete hardware recommendations and file system supported, refer to the *Mobility Unified Reporting System Overview* chapter in the *Cisco Mobility Unified Reporting System Installation and Administration Guide*. For the OS installation information, refer to the *Cisco MITG RHEL v5.5 OS Application Note*.

IMPORTANT

The Cisco MITG RHEL v5.5 OS is a custom image that contains only those software packages required to support compatible Cisco MITG external software applications. Users must not install any other applications on servers running the Cisco MITG v5.5 OS. For detailed software compatibility information, refer to the *Cisco MITG RHEL v5.5 OS Application Note.*

Scheduling Offline BS/KPI Reports

On selecting multiple counters/indices or a huge data range on the Bulkstats and KPI reporting pages, the MUR server may experience some delay in fetching the report information. If the time taken for this activity is beyond the expected threshold, then these tasks are automatically scheduled to be reported offline at a later period.

An automated offline script at the server side runs every 1 minute to check if the requested report information is available. When it is ready, the server makes it available on **Background Task Manager** tab present on the GUI. These offline reports are generated in Excel format and provided to users as a zip file.

Search Facility for BS Counters

The current release of MUR allows users to search the bulkstats (BS) counters using the **Counters** text box newly added in the Bulkstats reporting page, and also find the CLI-equivalent counter names by selecting **by CLI Name** check box.

With the auto-complete feature available in the **Counter** text box, you can just key in a few characters and search the counters easily.

Support for Configuring Multiple SGSN Groups

MUR users have been provided the flexibility to configure multiple SGSN IP addresses under one SGSN group using “ * ”. The SGSN group configuration can be performed on the GUI through **System > Reports > SGSN groups** menu.

Users can now add explicit IP address expressions similar to the example shown here:

10.4.1.*

1*.4.1.74

10.4.*.74

.1..74

10.4.1.7*

10.4.1.*4

etc.

Support for Enabling KPI Parser

MUR architecture is redesigned so that KPI parser and Bulkstats (BS) parser does not coexist and they function independently from release 12.0 onwards.

The KPI parser now calculates only the values of KPIs for which the alarms are configured through the GUI. This parser uses the information stored by BS parser in the database (DB) for KPI calculations and for sending alarms. This avoids reparsing of the same file and redundant connections to the DB.

KPI parser generates alarms only when the alarm functionality is enabled through the **SNMP Configurations** option available on the GUI under the **System** menu.

MUR Features in Release 12.2

This section provides information on new Mobility Unified Reporting (MUR) features in Release 12.0.

Aggregation Support for Top N Subscribers Report

In this release, the Top N Subscribers Report and Top N VCD Subscribers Report are available per week and month.

E-mailing Capabilities of MUR

Apart from custom reporting, the support for e-mailing weekly/monthly reports and all alarms including KPI alarms is made available in this release.

If the user(s) and e-mail server are configured in MUR,

1. Weekly Reports and Monthly Reports URL will be e-mailed to configured e-mail users at the start of the week and at the start of the month
2. If MUR alarms are enabled then KPI alarms are e-mailed to configured users

MUR Installer Changes

In this release, a new parameter "**Available Port Range for MUR Components (200 Ports)**" has been introduced during the MUR installation. With this parameter, the user can either accept the default port range or enter a new port range when the default ports are not available.

Please note that the user is required to enter only the start port number as the end port number will be populated automatically based on the start port number. If any of the port/ports in the specified range is/are busy then the installer throws error and prompts the user to enter new start port number.

MUR Support for Tethering Detection

The ASR chassis works in conjunction with the MUR application to facilitate tethering detection on the chassis. The EDRs generated by the chassis will be enhanced to include OS signatures.

IMPORTANT

Use of Smartphone tethering detection feature requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

MUR processes flow-EDR files containing OS signature and IMEI field, HTTP files containing User Agent and IMEI field, and populates the following set of data in the respective database files.

- Laptop (USB Dongles device group) - User Agent data - Identifies the browser from which the HTTP or WAP request is generated from.
- Laptop (USB Dongles device group) - OS Signature data - Applications and Operating systems running on the smartphone are device-specific
- Smartphone - IMEI/TAC data - Unique identifier for a device

MUR allows the user to enter dongle TACs through the GUI. This in turn allows MUR to identify all laptop OSs and Laptop UAs in the network by mapping the user identified dongle TACs to the corresponding laptop OS and laptop UAs for a flow. All other TACs could either be smartphone TACs or simplephone TACs. If MUR finds a laptop OS or laptop UA matching to a smartphone TAC, MUR will mark the flow as tethered and put into a tethered DB file. These database files are then pushed to all gateways under the */hd-raid/databases/* directory immediately or at a configurable intervals.

MUR provides the required data for tethering detection to the chassis. ECS software running on the chassis plays a vital role in the tethering detection. For information on how the detection is performed, see the *Enhanced Charging Services Administration Guide*.

Tethering Detection Database File Location - Behavior Change

The directory path to store Tethering Detection databases has changed.

Previous Behavior: In earlier 12.2 releases, the path to store the Tethering Detection database files was “/mnt/hd-raid/data/databases/”.

New Behavior: Now the path to store the tethering database files is “/hd-raid/databases/”.

New EDR Attributes for MUR Reporting

The EDR attribute “sn-volume-amt” reports the total uplink/downlink packets/bytes during a flow. This also contains the packets/bytes dropped and retransmitted by ECS.

With the use of “sn-volume-amt” counters, the report may not be an accurate representation of the packets/bytes actually downloaded by the subscribers. This might result in over-charging or over-reporting (the volume) of the subscribers.

To avoid this scenario, in this release, MUR supports the following new EDR attributes:

- sn-charge-volume ip bytes downlink
- sn-charge-volume ip pkts downlink
- sn-charge-volume ip bytes uplink
- sn-charge-volume ip pkts uplink

MUR provides the flexibility to choose among legacy “sn-volume-amt” or newly added counters “sn-charge-volume” to count the volume. By default, MUR will use “sn-volume-amt” to count the volume.

Region-based Reporting

In 12.0 and earlier releases, RDP was considered as a region. So, all reports were based on RDP. Whenever an RDP is configured, internally MUR used to create corresponding region for the same. However, in release 12.2 and beyond, one gateway's files will be processed by two or multiple RDPs. In that case, RDP does not stand as a region. So, reports will be required across all the RDPs under one specific region.

Particularly, when there are multiple such regions where each region has more than one RDPs, this feature becomes more important. A different case for the requirement of this feature is a region where there are multiple gateways and they are processed by different RDPs. In that case, per RDP based reports will not make sense, rather, region based reports will be required.

In this release, MUR allows users to create individual regions, and add RDPs to those regions. All the gateways must be associated with RDP(s) or NOC and not to a region.

Subscriber Data Storing and Reporting

MUR will now support 'Offline Subscriber Search Only' mode. In this mode, MUR will not parse the incoming EDR data and no GUI reports will be available. 'Offline Subscriber Search Only' MUR will move files directly to archive directory. It will be organized daily in this location. To switch to this mode, after installation, Go to **System** > **ConfigParameters** and change paramvalue of OFFLINE_MODE to True.

It is recommended for OFFLINE_MODE MUR to use more number of processes. The maximum number of processes is 30 per reporting type (total 60) considering a 64 core UCS machine.

Subscriber Search Enhancement

Along with the support for string-based MSISDNs (called as NAI: Network Access Identifier) of HA/PDSN (CDMA), subscriber search has been enhanced to include options to search by more dimensions like IMEI, Subscriber Port, etc.

The MUR GUI provides user with options to select type of search dimension as well as fields/columns that will appear in excel report. For example, user can select Search By MSISDN for searching subscribers having numeric MSISDNs, NAI for searching subscribers having string-based MSISDNs of HA/PDSN (CDMA).

Based on the reporting requirements, the user can add/remove the EDR fields from **Optional Fields** list to **Report Fields** list. Users can request an e-mail with report attached, while entering a search request.

The mandatory fields present at the time of search will be included in output CSV report. The fields applicable to flow EDRs will be present in flow CSV report. Fields applicable to HTTP EDRs will be present in Http CSV report.

Support for Additional Ports and Numerous P2P Protocols

MUR supports additional ports, as listed on IANA site, starting from 0 to 1600 and each of them are mapped to respective protocols.

In this release, MUR allows the user to select from the available port range at the time of installation.

Support for Granular Reporting

The granularity of access controls to user is being extended to ensure that access to reports is controllable by the user. This implies that the user is allowed to configure the granularity settings based on which the reports will be generated in real-time. For example, if granularity 5 is configured, then data will be parsed and report will be viewed with 5 minutes granularity.

The EDRs are processed as frequently as possible allowing reports to be generated shortly after the period to which they apply. Granularity support is currently provided for DPI and HTTP Content Type Summary reports.

Support for Meebo Protocols

MUR makes the MEEBO video/voice protocol available as P2P protocols by default. The meebo-audio is now mapped to voip, meebo-video to video and meebo-unclassified to streaming category.

Support for New Reports

In this release, MUR supports generation of the following new reports:

- Reports based on HTTP Services: This feature extends the definition of a service from host name to include a URL or part of a URL and/or port number. HTTP services can be defined as a combination of Host name, Content type, and Part of URL.
- Reports on Top N Device groups *vs* Top N Hosts and vice-versa: These reports are possible from the MUR GUI through HTTP tab and Custom Reporting option under Available Reports menu.
- Video Usage Monitoring Report: Through this custom TopN reporting feature, it is possible to monitor and report the video traffic usage as and when needed. This report is mainly required to identify TopN hosts for video traffic and also to determine the biggest sources of video traffic, which drives the network load at a greater extent.

  HTTP content type will be used to identify the video traffic. Ideally video traffic should be derived from flow-EDRs. Since the video usage monitoring report is generated based on HTTP content type, only HTTP traffic will be counted.
- Report based on Cell Location: This feature allows the usage to be reviewed by Cell ID either as a Top N list of usage by location or a list of fixed locations to be monitored (for top N subscribers per cell) or as a filter on reports (comparable to SGSN group or Device group).

  On selecting Location Group filter from the Filter selection panel, the following reports can be derived:

  - Location by volume
  - Cell per location by volume

  TopN subscribers per cell report can also be generated but through the TopN Search tab under Custom Reporting.
- Report for Roaming Monitor: The concept of “Roaming Partner Group” is introduced for this reporting. Roaming partner can be defined using MCC-MNC pair as well as SGSN group. Each roaming partner can have multiple MCC-MNC pairs and SGSN groups.

  MUR users should manually configure MCC and MNC through System menu, and then map this MCC-MNC combination with the roaming partner.
- Reports based on HTTP Service Profile: Service Profile is defined as the group of rulebases. Hence, for the service profile reports to be fetched, rulebase name is the mandatory input required from the user. The “Rulebase” name should be added and then a Service Profile must be created to map with the rulebases.
- Report on Top N Unknown Ports: This report highlights the top N ports for which traffic is classified as either unidentified or unknown. This report can be viewed through the link **Edr unknown port infos** under the **System** menu.

- Reports based on Session: This report provides the statistical analysis of user sessions over the session duration. A session is defined as the unique combination of GGSN address and charging identifier. Charging identifier is used together with GGSN address to identify all records produced in SGSN(s) and GGSN involved in a single PDP context.

Support for P2P Video Detection

MUR now supports traffic type detection for P2P protocols such as Skype, Gtalk, MSN, Yahoo, and Oscar with the use of “traffic-type” attribute present in the EDR fields. Based on the value of this EDR attribute, the data will be classified to respective protocols.

Support for TopN HTTP Hosts Report

TopN IP Traffic Report is no longer supported. MUR now supports TopN HTTP Hosts report, which can be used instead. This report uses “ip-server-ip-address” Flow-EDR attribute.

In the XLS report, TopN IP worksheet will be empty.

MVG Features in Release 12.0

The Mobile Video Gateway is a new product in Release 12.0.

For information about the Mobile Video Gateway, see the *Mobile Video Gateway Administration Guide*.

MVG Features in Release 12.2

This section provides information on new Mobile Video Gateway features in Release 12.2.

MVG Support on the GGSN

In Release 12.2, the Mobile Video Gateway software can be integrated with a GGSN (Gateway GPRS Support Node) in a GPRS/UMTS (General Packet Radio Service/Universal Mobile Telecommunications System) network.

For more information, see the *Mobile Video Gateway Administration Guide* for Release 12.2.

NAT Features in Release 12.0

This section provides information on new Network Address Translation (NAT) features in Release 12.0.

Support for H323 ALG

This release provides support for H323 ALG that is designed to traverse NAT by inspecting and altering information contained in existing H323 messages as they pass through the NAT. It can alter address and port information in registration, call signaling and automatically opening pinholes in the NAT to allow media flow.

H323 ALG performs the following functions:

- Communicates with the core for binding management
- Uses H323 stack for parsing and encoding the H323 messages
- Communicates with NAT for signaling messages
- Performs protocol specific processing if required

Supplementary Services

The following supplementary services are currently supported in H323 ALG:

- Call Transfer: The Call Transfer supplementary service enables the served user (User A) to transform an existing call with a User B (primary call) into a new call between current User B and a new User C (transferred-to user) selected by served user A.
- Call Hold: The Call Hold supplementary service allows the served user, which may be the originally calling or the called user, to interrupt communications on an existing call and then subsequently, if desired, re-establish (i.e. retrieve) communications with the held user.
- Call Diversion: Call Diversion supplementary service permits a served user to have incoming calls addressed to the served user's number redirected to another number; on busy service, it enables a served user to have calls redirected to another endpoint; on No Answer, it enables a served user to have calls addressed to the served endpoint's number and redirected to another endpoint if the connection is not established within a defined period of time.
- Call Waiting: The Call Waiting supplementary service permits a busy user to be informed of an incoming call while being engaged with one or more other calls.
- Call Offering: The Call Offering supplementary service on request from the calling user, enables a call to be offered to a busy user and to wait for that called user to accept the call, after the necessary resources have become available.

NAT Aware H323 Clients

An application layer gateway, at the Firewall/NAT, examines all the H323 packets and modifies the packet such that all the private addresses are replaced by public addresses. It also opens all the pinholes required for successful call establishment. A NAT aware endpoint establishes end-to-end media session through FW/NAT without the need of ALG. Any TCP connection or UDP packet sent from the internal network through the firewall opens a pinhole dynamically in the firewall. This pinhole allows incoming messages to be sent from the destination of the TCP connection or the UDP packet. The pinhole stays open as long as the network sends information through the pinhole to the same destination.

If an end point supports NAT traversal, H323 ALG disables itself so that end point directly opens required pinhole and establishes media path between them. The ALG will not manage any pinhole for media traversal across Firewall/NAT for NAT aware clients. By default, the ALG will bypass all the clients that support H460.18/19 and H460.23/24.

For more information, see the *Network Address Translation Administration Guide*.

NAT Features in Release 12.2

This section provides information on new Network Address Translation (NAT) features in Release 12.2.

Support for NAT64

Stateful NAT64 is a mechanism for translating IPv6 packets to IPv4 packets and vice-versa. The IPv4 address of IPv4 server/host in an IPv4 network is obtained to and from IPv6 addresses by using the configured stateful prefix. The IPv6 addresses of IPv6 hosts are translated to and from IPv4 addresses by installing mappings in the usual NAT manner.

NAT64 is applied on traffic based on the rule match (Destination based NATing). If NAT64 has to be applied, then the NAT64 will translate and forward them as IPv4 packets through the IPv4 network to the IPv4 receiver. The reverse takes place for packets generated by hosts connected to the IPv4 network for an IPv6 receiver. If NAT64 is not applied on the IPv6 packet, then the IPv6 packet will not be translated and sent as is (NAT bypassed) and will be routed within the IPv6 network to the destination.

NAT64 will not be applied for packets whose destination IP address does not match a pre-defined prefix. NAT64 will be applied only for packets whose destination IP address matches a pre-defined prefix. The pre-defined prefix is configurable, and it can be a single prefix or a group of prefixes.

Support for NAT64 ALGs

NAT64 ALGS support the following protocols:

- File Transfer Protocol (FTP)
- Point-to-Point Tunneling Protocol (PPTP)
- Real Time Streaming Protocol (RTSP)
- Trivial File Transfer Protocol (TFTP)

ICSR Support

This release now supports the following:

- Many-to-one NAT flow recovery in ICSR
- SIP ALG supports ICSR and is applicable only to UDP flows

For more information, see the *Network Address Translation Administration Guide*.

PDG/TTG Features in Release 12.0

This section provides information on new PDG/TTG features in Release 12.0.

None for this release.

PDG/TTG Features in Release 12.2

This section provides information on new PDG/TTG features in Release 12.2.

Lawful Intercept

TCP Proxy Support

TCP Proxy support is now available for Lawful Intercept on the PDG/TTG. Contact your local sales representative for detailed information.

Notification of LI Target Provision Modification/Deletion

The PDG/TTG now supports the sending of a notification to LI administrators when an existing LI target provision has been modified or deleted. Contact your local sales representative for detailed information.

PDIF Features in Release 12.0

This section provides information on new Packet Data Interworking Function (PDIF) features in Release 12.0.

None for this release.

PDIF Features in Release 12.2

This section provides information on new Packet Data Interworking Function (PDIF) features in Release 12.2.

None for this release.

PDSN Features in Release 12.0

This section provides information on new Packet Data Serving Node (PDSN) features in Release 12.0.

None for this release.

PDSN Features in Release 12.2

Lawful Intercept

TCP Proxy Support

TCP Proxy support is now available for Lawful Intercept on the PDSN. Contact your local sales representative for detailed information.

Notification of LI Target Provision Modification/Deletion

The PDSN now supports the sending of a notification to LI administrators when an existing LI target provision has been modified or deleted. Contact your local sales representative for detailed information.

Support for Transfer of LI Information in TCP Format

The PDSN now has the capability to send intercepted information in TCP format. Contact your local sales representative for detailed information.

P-GW Features in Release 12.0

This section provides information on new Packet Data Network Gateway (P-GW) features in Release 12.0. Additional information on these features can be found in the *Cisco ASR 5000 Series Packet Data Network Gateway Administration Guide* and the *Cisco ASR 5000 Series Command Line Interface Reference.*

3G Access to GGSN-PGW-R8 - Gx Bearer ID Missing

Previous Behavior

In case when UE_ONLY BCM was received from PCRF, IMSA terminated the call for P-GW/GnGp P-GW because BCM of UE_ONLY was not supported.

New Behavior

When BCM of UE_ONLY is received from PCRF, P-GW/GnGp P-GW will not terminate the call. This is applicable to all dictionaries.

New **`policy-control bind-default-bearer`** CLI command will bind all the PCC dynamic or pre-defined rules coming from PCRF to the default bearer in the following circumstances:

- no QCI
- QCI that matches the default bearer, but no ARP defined
- QCI and ARP that matches the default bearer.

This CLI will be used when BCM mode is UE_ONLY.

If the P-GW gets a rule with QCI/ARP other then the default bearer, it will ignore such rules and send a response that the rule could not be installed.

This command will not work for dedicated bearers (secondary PDP contexts). If the P-GW gets a PCC dynamic rule, pre-defined rule from PCRF with QCI or ARP different from that of the default bearer, then those rules will be dropped. Secondary bearers initiated by UE will not be supported.

3GPP-SGSN-MCC-MNC AVP Missing Within RADIUS Account

The attribute 3GPP-SGSN-Mcc-Mnc is now included in RADIUS Account records in dictionary custom15.

The attribute is also now seen in Access-Req message.

ARP Command Extended

Implemented changes to extend the existing CLI command for **`allocation-retention-priority`** to also optionally include enabling of PCI and PVI flags.

If these are not enabled explicitly, then the current values will hold true [PCI = 1, PVI = 0].

Charging Rulebase Name in LOSDV is Configurable

The maximum length of the charging rulebase name in List of Service Data Volumes (LOSDV) of P-GW CDRs can be trimmed now with the inclusion of new command **`gtpp egcdr rulebase-max-length <`***`rulebase_name_max_length`***`>`**. With this new command, user will have the flexibility to decide the length of charging rulebase name. The user needs to specify the rulebase name length explicitly, between 1 to 63, in LOSDV to use this feature. In case zero is specified, the charging rulebase name would not be trimmed.

For more information, refer the *Context Configuration Mode Commands* or *GTPP Group Configuration Mode Commands* chapter of the *Command Line Interface Reference Guide*.

ChargingRuleBaseName in P-GW CDRs

Previous Behavior

RuleBase attribute was sent as it is on the P-GW CDRs without trimming to 16 characters.

New Behavior

For GTPP dictionary custom40, RuleBase attribute name is trimmed to 16 characters in P-GW CDRs.

Diameter AVP Behavior Change

Formerly, insignificant zeroes in the monitoring key were stripped off while encoding/decoding it over Gx.

Now, insignificant zeroes are not stripped off while encoding/decoding the monitoring key AVP over Gx. As monitoring key is internally interpreted as an unsigned integer and the insignificant zeroes are not stripped off from the key, the value should be of four bytes in length and not lesser or greater; this will prevent PCRF rejection due to invalid length.

Direct Tunnel Support

When Gn/Gp interworking with pre-release 8 (3GPP) SGSNs is enabled, the GGSN service on the P-GW supports direct tunnel functionality.

EPC Combination Gateway Supports LTE requirements

The SGSN/GGSN, when co-residing with the S-GW/P-GW, supports all product-level requirements of the S-GW/P-GW for availability, performance, capacity, security, and O+M.

EPC Gateways Support for eHRPD Non-optimized Handoffs

This functionality has been implemented.

Generic APN Based on Routing Mechanism – IPSec Connection Method

This functionality has been implemented.

Gn/Gp Handover Behavior Change

In case of P-GW with GnGp access, after a P-GW mode to GGSN mode handover, SGSN_CHANGE(0) Event trigger and 3GPP-SGSN-Address needs to be sent. The system shall send AN_GW_CHANGE (21) Event-Trigger and IPv4 SGSN address in the AN-GW-Address AVP. This is because SGSN-Address would not have been valid in the case of P-GW with S5/S8 and, hence, SGSN_CHANGE(0) would not be meaningful after a P-GW mode to GGSN mode handover.

GRE Protocol Interface Support

The P-GW supports GRE generic tunnel interfaces in accordance with RFC-2784, Generic Routing Encapsulation (GRE). The GRE protocol allows mobile users to connect to their enterprise networks through GRE tunnels.

GRE tunnels can be used by the enterprise customers of a carrier 1) To transport AAA packets corresponding to an APN over a GRE tunnel to the corporate AAA servers and, 2) To transport the enterprise subscriber packets over the GRE tunnel to the corporation gateway.

The corporate servers may have private IP addresses and hence the addresses belonging to different enterprises may be overlapping. Each enterprise needs to be in a unique virtual routing domain, known as VRF. To differentiate the tunnels between same set of local and remote ends, GRE Key will be used as a differentiation.

GRE tunneling is a common technique to enable multi-protocol local networks over a single-protocol backbone, to connect non-contiguous networks and allow virtual private networks across WANs. This mechanism encapsulates data packets from one protocol inside a different protocol and transports the data packets unchanged across a foreign network. It is important to note that GRE tunneling does not provide security to the encapsulated protocol, as there is no encryption involved (like IPSec offers, for example).

GRE Tunneling consists of three main components:

- Passenger protocol-protocol being encapsulated. For example: CLNS, IPv4 and IPv6.
- Carrier protocol-protocol that does the encapsulating. For example: GRE, IP-in-IP, L2TP, MPLS and IPSec.
- Transport protocol-protocol used to carry the encapsulated protocol. The main transport protocol is IP.

IMPORTANT

This feature is license dependent. Please contact your local sales representative for more information.

GTP-U Data Forwarding Changes for IPSec

Sessmgrs are now informed of IPSec tunnels to peers.

GTP-U IPSec Peer Updates to sessmgr

gtpumgr now receives IPSec tunnel notifications from IPSec. gtpumgr now updates all sessmgrs with NPU flow information for the tunnel that is received from IPSec.

gtpumgr also notifies all sessmgrs of peer info. so that when any bearer setups for that peer, corresponding IPSec tunnel info. is used for data forwarding.

GTP-U IPSec Tunnel Create and Status Handling

If IPSec is enabled and a new peer is detected, a new IPSec tunnel is now initiated.

GTP-U Echoes Sent through IPSec Tunnel for a Peer Once the IPSec Tunnel to the Peer is Set Up

This functionality has been implemented.

Gtpumgr Restart Handling

With IPSec tunnels, if gtpumgr restarts, the IPSec tunnel info is now synced up with the IPSec subsystem and sessmgr.

Gy: Added CHANGE_IN_SERVING_NODE Trigger Type

CHANGE_IN_SERVING_NODE trigger is an extension to the CHANGE_IN_SGSN trigger. However, for the purpose of backward compatibility, both triggers are retained. The P-GW sends them in the following manner.

- If OCS does not provide any trigger:
  - SERVING_NODE AND SGSN is configured on the CLI, system sends SERVING_NODE_CHANGE.
  - If one of them is configured, that one will be sent.
- If OCS provides SERVING_NODE and SGSN, then CHANGE_IN_SERVING_NODE would be sent.
- If OCS provides:
  - SGSN alone (older OCS), then the current behavior of sending CHANGE_IN_SGSN_IP_ADDRESS trigger is retained.
  - SERVING_NODE alone (newer OCS), then the new trigger CHANGE_IN_SERVING_NODE would be sent.

Gy: [GTP] Support for Generating SERVING_ NODE_CHANGE Trigger

This functionality has been implemented.

Gy: [PMIP] Support for Generating SERVING_ NODE_CHANGE Trigger

This functionality has been implemented.

ICSR Checkpointing

MSCC (quota) checkpointing is now handled as part of normal session recovery. MSCC checkpointing occurs randomly (~ 1-2 times within every 60 seconds) on every MSCC update. The MSCC checkpoint will be sent to the peer chassis only if there is a change in MSCC information.

IKEv2 IP Security Support on S5 Interface

IP Security (IPSec) on the S5 interface is a node-to-node IKEv2 tunnel that can be configured to assume the characteristics of either a pre-configured tunnel or a dynamic tunnel.

Pre-configured node tunnels are fully qualified IPSec tunnels. Each IPSec tunnel is configured with parameters including pre-shared key, local and remote IP addresses, crypto hashes, groups, algorithms and the access control list (ACL).

Node-to-node dynamic tunnels are generated dynamically as the connections are initiated by different nodes in the LTE network. Each IPSec tunnel does not need to be pre-configured for each required parameter, instead it uses a common template for some parameters, like crypto algorithms, hashes, and groups. Other parameters are fetched dynamically from the tunnel requests like IP addresses and traffic selectors. Authentication information is fetched dynamically via certificates.

Typically, the S-GW initiates an IPSec tunnel to the P-GW. The P-GW service is responsible to verify the configuration and use an IPSec API to make the P-GW listen on the service address for IKE requests.

When configured for IPSec, the S5 Interface carries GTP-C signaling traffic and GTP-U data traffic that flows through an IPSec tunnel.

IPSec Tunnel Deletion for a Peer If No Bearers are Present for That Peer

IPSec tunnels are now deleted for a peer if no bearers are present for that peer.

Local QoS Policy

Local QoS policies can be used to control different aspects of a session, such as QoS, Data Usage, Subscription profiles, or Server Usage, by means of locally defined policies.

Local QoS policies are triggered when certain events occur and the associated conditions are satisfied. For example, when a new call is initiated, the QoS to be applied for the call could be decided based on the IMSI, MSISDN, and APN.

IMPORTANT

This feature is license dependent. Please contact your local sales representative for more information.

LTE IPSec Scaling Support

This functionality has been implemented.

LTE IPSec Single Tunnel Set Up for Both Initiator and Responder

S-GW acts as Initiator and Responder toward eNodeB.

Toward P-GW, there is collision scenario when S-GW and P-GW both initiate a tunnel at the same time; however, one of them will terminate.

NEMO Service Supported

The P-GW may be configured to enable or disable Network Mobility (NEMO) service.

When enabled through a feature license key, the system includes NEMO support for a Mobile IPv4 Network Mobility (NEMO-HA) on the P-GW platform to terminate Mobile IPv4 based NEMO connections from Mobile Routers (MRs) that attach to an Enterprise PDN. The NEMO functionality allows bi-directional communication that is application-agnostic between users behind the MR and users or resources on Fixed Network sites.

The same NEMO4G-HA service and its bound Loopback IP address supports NEMO connections whose underlying PDN connection comes through GTP S5 (4G access) or PMIPv6 S2a (eHRPD access).

IMPORTANT

This feature is license dependent. Please contact your local sales representative for more information.

On sessmgr Restart/Start, GTP-U Peer Info Fetched from gtpumgr

This functionality has been implemented.

P-GW Supports Average Throughput Per Active User of 10 Kbps on Uplink and 50 Kbps on Downlink

The P-GW service now supports average throughput per active user of 10 Kbps on uplink and 50 Kbps on downlink.

P-GW Supports DHCP Relay Over SGi Per-APN IPSec Tunnel

The P-GW service now supports DHCP relay over SGi per-APN IPSec tunnel.

P-GW Supports Throughput Per Active Video Streaming User Device of 256Kbps on Uplink and 1Mbps on Downlink.

The P-GW service now supports throughput per active video streaming user device of 256Kbps on uplink and 1Mbps on downlink.

PSC3 Hardware Support

The P-GW service supports the use of the Packet Service Card 3 in this release.

QCI Range Changed

Previously, for Default-EPS-Bearer QoS, IMSA validation for QCI ranges 1-9 and 128-254 were considered valid (as per spec).

Now, the valid QCI range has been changed to 1-32 to align with the CLI configurable range.

S-GW and P-GW Support Secure User Plane Interfaces Using IPSec

IKEv2 has been implemented for Node-to-Node IPSec Tunnels in the LTE network for GTP-U traffic.

The IPSec implementation for LTE is only node-to-node. Any IPSec tunnel will handle multiple subscriber GTPU traffic. The IPSec tunnel is generated dynamically as the connection is initiated by nodes in the LTE network. Each IPSec tunnel uses a common template for parameters, such as crypto algorithms, hashes, groups, etc. Other parameters are fetched dynamically from the tunnel requests, such as IP addresses and traffic selectors. Authentication information is fetched dynamically via certificates.

For LTE nodes, IPSec tunnels can be setup for control and data traffic carried over S1-MME, S1-U, S11, and S5.

SNMP Notification on Configuration Change

The configuration monitor utility will perform a show configuration command every 15 minutes and compare the subsequent output to determine whether the information has changed. The configuration is defined as having changed when the current configuration

differs from the previous snapshot. If a configuration change is indicated, then an SNMP trap is sent.

Support for Event Trigger UE_IP_ADDRESS_ ALLOCATE and UE_IP_ADDRESS_RELEASE

Added support for displaying event-masks and statistics for Event-Triggers UE-IP-Address-Allocate and UE-IP-Address-Release.

X.509 Certificate-based Peer Authentication

The P-GW supports X.509 certificate-based peer authentication for IPSec tunnels over the S5 interface.

P-GW Features in Release 12.2

This section provides information on new Packet Data Network Gateway (P-GW) features in Release 12.2. Additional information on these features can be found in the *Cisco ASR 5000 Series Packet Data Network Gateway Administration Guide* and the *Cisco ASR 5000 Series Command Line Interface Reference.*

1:1 NAT64 Not Happening if NAT44 Initiated First and Vice Versa

Previous Behavior

1:1 NAT IP was either used for NAting IPv4 or IPv6 traffic, but not both. There was no 1:1 NAT64 binding table. All downlink traffic received on 1:1 NAT64 IP was translated to client IPv6 address in ACL clp, irrespective of the interface id used for uplink.

New Behavior

1:1 NAT IP can be shared by IPv4/IPv6 traffic. 1:1 NAT64 binding table is maintained to store the interface ID/prefix. The downlink traffic is properly translated based on the binding table. The interface ID/prefix are obtained form the binding entry.

1:1 NAT 64 will now function as expected.

3GPP2-BSID AVP sent on Gx Interface

The support for sending BSID in CCR I and CCR U for LTE to EHRPD handoff is now working as expected.

Previous Behavior

Prior to the change, 3GPP2-BSID was not supported in Gx messages sent out for eHRPD.

New Behavior

3GPP2-BSID will be sent in Gx messages in the following cases:

- CCR-I at Session Creation Time.
- CCR-U when there is a hand off from LTE to EHRPD.

Accurate UE Time Zone Reporting

Verified that P-GW is able to process UE time zone IE from S5/S8 from MME/S-GW. Also, P-GW-PCRF interaction has been verified.

Always-On Licensing

Traditionally, transactional models have been based on registered subscriber sessions. In an “always-on” deployment model, however, the bulk of user traffic is registered all of the time. Most of these registered subscriber sessions are idle a majority of the time. Therefore, Always-On Licensing charges only for connected-active subscriber sessions.

A connected-active subscriber session would be in “ECM Connected state,” as specified in 3GPP TS 23.401, with a data packet sent/received within the last one minute (on average). This transactional model allows providers to better manage and achieve more predictable spending on their capacity as a function of the Total Cost of Ownership (TCO).

Bearer Modification Reject by P-GW Causes “No resources available”

In the case of 4G to 3G handover P-GW retained the ARP value of the call. The GGSN after 4g to 3g handover had a different value for ARP. Due to this, MME sent a different value of ARP in 3G to 4G handover in the create session request to S-GW. Now, S-GW had a different value for ARP than P-GW. Therefore, the MME sent a modified bearer command to the P-GW since the P-GW retained the ARP value from the initial value for the ARP when the call was on 4G.It sent a modified bearer failure indication to MME.

When MME sends a modified bearer command with same bearer_qos and APN AMBR that P-GW already has, the P-GW will now send an updated bearer request to the S-GW instead of sending the modified bearer failure indication to MME.

Previous Behavior

If bearer_qos and APN-AMBR received a modified bearer command that was the same as the bearer_qos and the APN-AMBR that the P-GW already had, then the P-GW sent a modified bearer failure indication to MME.

New Behavior

If bearer_qos and APN-AMBR receives a modified bearer command that is the same as bearer_qos and the APN-AMBR that P-GW already has, then P-GW will send an updated bearer request to the S-GW instead of sending a modified bearer failure indication to MME.

CLI Command “show ims-authorization” Output Corrected

Previous Behavior

Bearer ID was displayed as “0” in the output of CLI command **`show ims-authorization sessions all`** for all except access type 3GPP-GPRS.

New Behavior

Bearer ID is displayed as “NA” in the output of CLI command **`show ims-authorization sessions all`** for all except access type 3GPP-GPRS.

Configuration Changes to Allow Gy-based User Sessions to Continue During OCS Failure and Ability for P-GW/HA to Continue Data Session for Fixed Time/Quota During OCS Outage

Existing **`servers-unreachable`** command has been modified. If set, new configuration options would:

- Determine the gateway behavior if OCS becomes unreachable, either due to transport failure or due to message timeouts owing to network congestion.
- Control the triggering of server-unreachable scenarios at response timeout or at Tx expiry.
- Allow P-GW/HA to continue data session for fixed time/quota during OCS outage.

Dedicated Bearer Restrictions

Using local policies, the following procedures can be performed:

- Allow dedicated bearers for subscribers belonging to all PLMNs.
  - This is achieved by activating predefined rules on the PCEF.
- Allow dedicated bearers on a per PLMN basis (list must support at least 5 PLMNs).
  - Serving-PLMN can be used as a classifier to evaluate the condition.

EXAMPLE(S)

Allow dedicated bearers for all PLMNs

```
config
    local policy test
        ruledef all-plmn
            condition priority 1 serving-plmn match .*
        exit
        actiondef create-bearer
            action priority 1 activate-rule ded-bearer
        exit
        eventbase new-call
            rule priority 1 ruledef all-plmn actiondef create-bearer
        end
```

```
        exit
    end
```

Allow dedicated bearers on a per PLMN basis

```
    config
        local policy test
            ruledef select-plmn
                condition priority 1 serving-plmn eq 123.* 456.*
            exit
            actiondef create-bearer
                action priority 1 activate-rule ded-bearer
            exit
            eventbase new-call
                rule priority 1 ruledef select-plmn actiondef create-bearer
            end
        exit
    end
```

ECS Maximum Sessions Limit

Previous Behavior

Every bearer in a P-GW (or pdp context in case of GGSN) belonging to the same subscriber consumed one ECS license each. When a subscriber had multiple bearers/pdp contexts, then ECS licenses were exhausted before the actual limit for subscribers was reached, which resulted in new calls being denied.

New Behavior

Now, a single ECS license is consumed per subscriber, irrespective of the number of default or dedicated bearers (primary or secondary pdp contexts) it may have. ECS licenses will be exhausted only after reaching the configured limits.

Flow Definition Based on Domain Name

Added support for grp-of-ruledefs and predefined-dynamic-rule. Added DNS analyzer changes for storing IPv4, IPv6 and CNAME entries and removing the config lists on “no” CLIs. Added CLI command for adding **`ip server-domain-name`** ruledef and creating IP table per rulebase.

Functional Behavior Change for Prefix Len Value in IPv4 Home Address Reply Option in PBA

If CLI command **`ip pool`** has **`subscriber-gw-address`** configured, then value configured will be sent in IPv4 default router address option in PBA.

In addition, value of prefix len in PBA will be set to mask of the pool if **`mobility-option-type-value standard`** is configured in LMA service.

GTP-U Sequence Number

CLI command added to enable/disable addition of the sequence number to every GTP-U packet coming from Gi interface and going towards Gn/Gp interface. If GTP-U packets are received out of sequence, sequence numbers would allow the packets to be recorded.

Gx Interface Updates

- Support for IPv4 deferred address selection.
- Support for new Packet-Filter-Operation and Packet-Filter-Information AVPs.
- Support for sending 3GPP-MS-Time Zone.
- Support for Event Trigger related AVPs in RAA.
- Support for Flow-Information in Charging Rule Definition.

Gy Feature Parity

Custom dictionary added to support the following features developed for the Home Agent DCCA Gy:

- Conveying of User Location Information to OCS for all RAT types
- Conveying of RAT type info to OCS
- Conveying of SGSN IP address to OCS
- Support of DCCA redirection
- Support of default quota
- Support of DCCA failure handling action=continue with timer (allow session to continue and disconnect after timer)

IMSI+CC Based Virtual APN Selection

Previous Behavior

With previous **`virtual-apn`** CLI command, either cc or imsi could be used to define a selection rule for virtual apn.

New Behavior

Now, **`virtual-apn`** CLI command can also be used to define a imsi+cc virtual apn selection rule.

Install Rules on Default Bearer Without Access Interactions

While installing the dynamic and predef rules in LTE scenario, if qci and arp values specified in the rule are of the default bearer, then TFT is not sent to MS. Also, if qci and

arp are not specified in the rule, then the configuration of the default bearer will be used and TFT is not sent to MS.

CLI Changes:

```
policy-control update-default-bearer
default policy-control update-default-bearer
```

These above configurations will continue sending TFT to the MS on default bearer.

```
no policy-control update-default-bearer
```

This configuration will not send TFT to MS on default bearer.

Interface ID Not Allowed in IPv6 Range Pools

Previous Behavior

CLI command **ipv6 pool <***name***> range <***start_address end_address***>** was allowing interface ID as part of configuration.

New Behavior

When interface ID part of the IPv6 address is configured as part of range, interface ID is cleared and a warning message is displayed.

Lawful Intercept

TCP Proxy Support

TCP Proxy support is now available for Lawful Intercept on the P-GW. Contact your local sales representative for detailed information.

Notification of LI Target Provision Modification/Deletion

The P-GW now supports the sending of a notification to LI administrators when an existing LI target provision has been modified or deleted. Contact your local sales representative for detailed information.

NAT Binding Updates (NBU) Supported on P-GW

This functionality has been implemented.

Node Selection: P-GW Selects OCS

P-GW may be configured with Diameter peer information for a pair of primary and secondary Online Charging Server (OCS). In this case, P-GW shall select the secondary OCS when the primary OCS is not available. P-GW shall perform an AAAA DNS query (IPv6) on FQDN (from Diameter peer information) to obtain the IP addresses of primary and secondary OCS nodes. P-GW shall then establish CER/CEA connectivity toward both

OCS nodes. For normal Gy Diameter Credit-Control Application (DCCA) requests, the P-GW shall use the primary OCS connection.

Option Required to Keep eGTP-C Sessions Alive After Echo Timeout

Previously, the system cleared all subscribers to the downed eGTP-C peer after echo timeout. This is still the default system behavior.

New CLI configuration has been added to allow the following alternate behavior in peer outage/restart scenarios:

1. When there is an eGTP-C timeout, log event, but do not clear subscribers.
2. When the peer comes back, only clear subscribers if the recovery/restart counter has been incremented on the peer.

P2P Local Pattern MyPeople Support in Customer PCEF

Completed the following CLI command changes as part of the P2P CLI implementation:

- **`show active-charging sessions`**
- **`show active-charging flows`**
- **`show active-charging flows`**
- **`show active-charging analyzer statistics`**

P-CDR Enhancements to Service and Rating IDs

The allowed range of **`content-id`** configurable was changed to maximum 31-bit value. The allowed range of **`service-identifier`** configurable was changed to maximum 31-bit value. The following CLI commands help text has been changed to display maximum value as 2147483647 instead of 65535:

- **`service-identifier <`***`value`***`>`**
- **`content-id <`***`value`***`>`**
- **`cca quota holding-time <`***`value 1`***`> content-id <`***`value 2`***`>`**

Previous Behavior: The maximum value allowed to be configured for **`content-id`** and **`service-identifier`** was 65535 (maximum 16-bit value).

New Behavior: The maximum value now allowed to be configured for **`content-id`** and **`service-identifier`** is changed to 2147483647 (maximum 31-bit value).

P-GW CDR Adaptation

custom42 is a new GTPP dictionary supporting ASCII format P-GW CDRs.

P-GW CDRs are locally stored on HDD.

The following events trigger closure and the sending of a partial P-GW CDR:

- every x octets configured using “volume x” (up/down/total)

A P-GW CDR is closed as the final record of a subscriber session for the following events:

- Detach Request received from UE
- Delete bearer context request received from S-GW.
- Manual subscriber clearing
- Abnormal Releases, such as path failures

P-GW Failed CRBN Change with GW_PCEF_MALFUNCTION

Previous Behavior

If default bearer QoS/APN AMBR change is reported in CCR-U but not authorized, the access side procedure is rejected in case of 3G call on P-GW.

New Behavior

If default bearer QoS/APN AMBR change is reported in CCR-U but not authorized, the access side procedure is not rejected in case of 3G call on P-GW.

P-GW RAR Handling While Waiting for CCA Issue for Gy OUT-OF-CREDIT

Previous Behavior

In the case when RAR was received from PCRF when there is a pending auth state, PCEF responded with a permanent failure (Unable to Comply). As per RFC 3588, the client/server should not retry the request if there is a permanent failure in a response. PCEF should not respond with permanent failure and instead let the PCRF retry the request after some time.

New Behavior

Since there are no transient failures fitting this category, using protocol error “Unable to Deliver”.

Range for ARP Value in Local Policy Increased

Previous Behavior

ARP had a range from 1-15.

New Behavior

ARP range increased to 1-127.

RAR handling in P-GW from OCS

1. If rating-group/service-identifier is received in RAR,
   - regardless of Gating Expire Time expiry, PCEF respond and shall immediately send CCR-U, Rating-Group/Service-Identifier, Reporting-Reason = forced_reauth.
   - if the corresponding service group is in denied state, Used-Service-Unit shall be set to 0.
   - if the corresponding service group is in active state, Used-Service-Unit shall be set to real value.
2. If rating-group/service-identifier is not received,
   - regardless of Gating Expire Time expiry, PCEF shall not send CCR-U
   - when user traffic comes and Gating Expire time expires, PCRF shall send CCR-U, Reporting-Reason = quota_exhausted
   - if the corresponding service group is in denied state, Used-Service-Unit shall be set to 0
3. Inter-RAT handover case:
   - PCRF shall send all the MSCCs for all the rating groups including denied rating groups
   - reporting-reason = Rating-Condition-Change
   - if the corresponding service group is in denied state, Used-Service-Unit shall be set to 0
   - if the corresponding service group is in active state, Used-Service-Unit shall be set to real value

Support at Minid

Support has been added in minidiameter to send Gating-Expire-Time AVP in response to CCR-FINAL (for FUA-Terminate and 4012 case).

Support at DCCA Level

mscc->grant.gating_expire_time is at mscc level and represent those MSCCs for which Gating-Expire-Time AVP was received from the server.

The timestamp is stored in:

time_t gating_expire_time /* and indicates the time for which PGW must have GATE-Off for gate-off services.*/

Release 9 3GPP References Supported

The P-GW currently supports the following Release 9 3GPP specifications. Most 3GPP specifications are also used for 3GPP2 support.

- 3GPP TR 21.905: Vocabulary for 3GPP Specifications
- 3GPP TS 22.115: Service aspects; Charging and billing
- 3GPP TS 23.003: Numbering, addressing and identification
- 3GPP TS 23.007: Restoration procedures
- 3GPP TS 23.060. General Packet Radio Service (GPRS); Service description; Stage 2
- 3GPP TS 23.203: Policy and charging control architecture
- 3GPP TS 23.207: End-to-end Quality of Service (QoS) concept and architecture

- 3GPP TS 23.216: Single Radio Voice Call Continuity (SRVCC); Stage 2
- 3GPP TS 23.228: IP Multimedia Subsystem (IMS); Stage 2
- 3GPP TS 23.401: General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access
- 3GPP TS 23.402. Architecture enhancements for non-3GPP accesses
- 3GPP TS 24.008: Mobile radio interface Layer 3 specification; Core network protocols
- 3GPP TS 29.060: General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface
- 3GPP TS 29.061: Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN)
- 3GPP TS 29.212: Policy and Charging Control over Gx reference point
- 3GPP TS 29.214: Policy and Charging control over Rx reference point
- 3GPP TS 29.229: Cx and Dx interfaces based on Diameter protocol
- 3GPP TS 29.230: Diameter applications; 3GPP specific codes and identifiers
- 3GPP TS 29.272: Evolved Packet System (EPS); Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol
- 3GPP TS 29.273: 3GPP EPS AAA Interfaces
- 3GPP TS 29.274: 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3
- 3GPP TS 29.275: Proxy Mobile IPv6 (PMIPv6) based Mobility and Tunnelling protocols; Stage 3
- 3GPP TS 29.281: General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U)
- 3GPP TS 29.282: Mobile IPv6 vendor specific option format and usage within 3GPP
- 3GPP TS 32.240: Telecommunication management; Charging management; Charging architecture and principles
- 3GPP TS 32.251: Telecommunication management; Charging management; Packet Switched (PS) domain charging
- 3GPP TS 32.298: Telecommunication management; Charging management; Charging Data Record (CDR) parameter description
- 3GPP TS 32.299: Telecommunication management; Charging management; Diameter charging application

Removed “violate-action shape” from “apn-ambr” Command

Added support for grp-of-ruledefs and predefined-dynamic-rule. Added DNS analyzer changes for storing IPv4, IPv6 and CNAME entries and removing the config lists on “no” CLIs. Added CLI command for adding **`ip server-domain-name`** ruledef and creating IP table per rulebase.

Rf Interface Updates

- In SDF level accounting, buckets are created and maintained using the Reporting-Level AVP value present in Gx message. The following are the accounting keys currently supported:
  - Rating-group
  - Rating-group and Service-Identifier
  - Rating-group and QCI
  - Rating-group, Service-Identifier, and QCI

  New CLI added in Accounting Policy Configuration Mode.
- Existing volume/time limit is applied for session level in accounting policy. New CLI configuration added at SDF level.
  - Service Data Volume Limit: Volume Limit reached for a specific flow. The container for this change condition will be cached by the P-GW and the container will be in an ACR Interim/Stop sent for partial record (Interim), final Record (Stop), or AII trigger (Interim) trigger.
  - Service Data Time Limit: Time Limit reached for a specific flow. The container for this change condition will be cached by the P-GW and the container will be in an ACR Interim/Stop sent for partial record (Interim), final Record (Stop), or AII trigger (Interim) trigger.

S5/S8 Interface Updates

- Updated mobility option type values for IPv4 Home Address, Address Acknowledgement, GRE Key, and Default Router options to the IANA assigned values.
- FTEID SGW_GTPU_INTERFACE_FOR_UL_DATA_FWD now 28.
- Trace info IE added in Identification Rsp.
- UE Timezone added in Forward Relocation Req and Context Rsp.
- Changes for supporting suspend/resume on S5/S8 interface.
- Indication IE is not 3byte. Changes include:
  - Monitor protocol changes
  - Encode/decode changes in indication IE

S6b Interface Updates

- PGW-Relocation-Indication AVP support added for S6b to support stale session notification/deletion.
- Assign static IP address over S6b support.
- S6b interface enhanced to pass the UE Assigned IP Address.
- S6b updated to define the IPv6 pool name AVP, and the P-GW supports the IPv6 pool name coming from AAA. Added support for Framed-IPv6-Prefix and Framed-Interface-ID.

Some AVPs Incorrectly Encoded in Gx Messages

Modified the Diameter dictionary.

Previous Behavior

"M" bit was set in some AVPs, violating the standard.

New Behavior

Removed the "M" bit in the following AVPs:

- Allocation-Retention-Priority
- AN-GW-Address
- APN-Aggregate-Max-Bitrate-DL
- APN-Aggregate-Max-Bitrate-UL
- Charging-Correlation-Indicator
- CoA-IP-Address
- CoA-Information
- Default-EPS-Bearer-QoS
- Event-Report-Indication
- Flow-Information
- Flow-Label
- Packet-Filter-Content
- Packet-Filter-Identifier
- Packet-Filter-Information
- Packet-Filter-Operation
- Pre-emption-Capability
- Pre-emption-Vulnerability
- Priority-Level
- Resource-Allocation-Notification
- Security-Parameter-Index
- Tunnel-Header-Filter
- Tunnel-Header-Length
- Tunnel-Information
- RAT-Type

The diameter incoming message parsing should take care of the absence of the "M" bit in these AVPs correctly.

Static Rules Applied Only to Default Bearers

Previous Behavior

Static rules should be applied only to default bearers. A check for this was missed in the DCCA init routine which decides whether a sub session is online charged by checking the “charging actions” of all static rules configured in the chassis and the installed pre-defined and dynamic rules.

New Behavior

Now, static rules are considered only for default bearers in the DCCA init routine. For dedicated bearers, only the charging actions of the installed pre-defined rules and dynamic rules decide whether DCCA needs to be enabled.

Supported-feature AVP in CCA from PCRF

Unless otherwise stated, the use of the Supported-Features AVP on the Gx reference point shall be compliant with the requirements for dynamic discovery of supported features and associated error handling on the Cx reference point.

The Supported Features here may have M bit set and Feature List ID and Feature List must not have “M” bit set.

Rel 8 is mandatory feature and does not mention the AVP flags for Feature-List-ID or Feature List.

Support for Stripping IMSI Prefix

TS 23.003, version 9.2.0, section 19.3.2 was updated as follows:

The NAI sent in the Mobile Node Identifier field in PMIPv6 will not include the digit prepended in front of the IMSI that is described above.

The current HSGW includes NAI received in EAP, and P-GW also expects this digit to be present. To support removing the leading digit, **`mobility-option-type-value standard`** configuration in MAG/LMA service will be used to support S2a MN-ID. There is no behavior change for **`custom1`** and it will continue to work as usual.

Added HSGW support for stripping IMSI prefix.

Completed P-GW changes to extract IMSI from NAI and handle cases when auth-mode digit is included or removed. **`mobility-option-type`** configuration is used and standard is expected to receive PBU without digit prepended.

In both HSGW/P-GW, PBU is expected to have <IMSI>@realm where IMSI field can only be maximum of 16 digits, including auth-mode. If it is more than 16 digits, then it is decoded as invalid IMSI format and IMSI will not be extracted.

In addition, **`mobility-option-type custom2`** configuration has been added for this feature. The standard will continue to work as before.

Traffic Shaping Not Supported for APN-AMBR

P-GW does not support traffic shaping for APN-AMBR. Therefore, the keyword **`shape`** and its options have been removed from the **`apn-ambr`** CLI command in the APN Configuration Mode.

UE Assigned Full IPv6 Address Reporting to AAA by P-GW

The P-GW needs to report the full IPv6 address assigned to the UE only. There is no need to report the IPv4 address, if assigned to the UE. The P-GW shall use Framed-IPv6-Prefix AVP to report the IPv6 prefix and Framed-Interface-Id to report the interface identifier (IID).

Virtual APN Selection Based on MSISDN Range and CC/RAT Type for P-GW

Parsed CC, RAT and MSISDN from incoming EGTP session create request.

Added EUTRAN RAT type in mapping function. Code for obtaining cc-profile from charging char IE.

VoLTE Based E911 Support

With this support, a UE is able to connect to an emergency PDN and make Enhanced 911 (E911) calls while providing the required location information to the Public Safety Access Point (PSAP).

E911 is a telecommunications-based system that is designed to link people who are experiencing an emergency with the public resources that can help. This feature introduces support for E911-based calls across the LTE and IMS networks. In a voice over LTE scenario, the subscriber attaches to a dedicated packet data network (PDN) called EPDN (Emergency PDN) in order to establish a voice over IP connection to the PSAP. Signaling either happens on the default emergency bearer, or signaling and RTP media flow over separate dedicated emergency bearers. Additionally, different than normal PDN attachment that relies on AAA and PCRF components for call establishment, the EPDN attributes are configured locally on the P-GW, which eliminates the potential for emergency call failure if either of these systems is not available.

Emergency bearer services are provided to support IMS emergency sessions. Emergency bearer services are functionalities provided by the serving network when the network is configured to support emergency services. Emergency bearer services are provided to normally attached UEs and to UEs that are in a limited service state (depending on local service regulations, policies, and restrictions). Receiving emergency services in limited service state does not require a subscription.

The standard (refer to 3GPP TS 23.401) has identified four behaviors that are supported:

- Valid UEs only
- Authenticated UEs only

- IMSI required, authentication optional
- All UEs

To request emergency services, the UE has the following two options:

- UEs that are in a limited service state (due to attach reject from the network, or since no SIM is present), initiate an ATTACH indicating that the ATTACH is for receiving emergency bearer services. After a successful attach, the services that the network provides the UE is solely in the context of Emergency Bearer Services.
- UEs that camp normally on a cell initiates a normal ATTACH if it requires emergency services. Normal attached UEs initiated a UE Requested PDN Connectivity procedure to request Emergency Bearer Services.

PCC Features in Release 12.1

The Policy and Charging Control (PCC) is a new product in StarOS Release 12.1.

The Cisco® ASR 5000 Platform provides 3GPP PPC solution to network carriers in UTRAN/E-UTRAN/cdma2000-1x/HRPD networks.

The Cisco PCC solution is based on 3GPP PCC model and standards, and intelligently extends it such as to simplify the complex and diverse requirements of policy and charging management for global operators.

The PCC solution comprises of Policy and Charging Rules Function (PCRF), Subscriber profile repository (SPR), and other interfacing module like Policy Provisioning Tool (PPT) to implement and control the policy based subscriber access in the existing wireless network as well as service flow based credit control implementation.

It includes the following functional entities:

- Intelligent Policy Control Function (IPCF)
- Subscriber Service Controller (SSC)
- Policy Provisioning Tool (PPT)

For information about the PCC solution, see the following guides:

- *Cisco ASR 5000 Series Intelligent Policy Control Function Administration Guide*
- *Subscriber Service Controller Installation and Administration Guide*
- *Policy Provisioning Tool Installation and Administration Guide*.

Policy Provisioning Tool in Release 12.1

Cisco Policy Provisioning Tool (PPT) is a Web-based client-server application which provides the user (network operator) a comprehensive use case design experience. It enables the network operator to design a service plan and subscriber profile data modelling at a time with the help of use case design and configuration.

PPT is designed to simplify use case configuration by importing the relevant Policy Control Enforcement Function (PCEF) flow, rules and APN data elements.

PCEF, typically located at the gateway is responsible for enforcing the policy and charging related decisions received from IPCF. PCEF performs service data flow detection as well as gate enforcement for the data flows.

For information about the PPT, refer *Policy Provisioning Tool Installation and Administration Guide.*

The PPT application is now supported on selected Cisco UCS servers running the custom Cisco MITG Red Hat Enterprise Linux (RHEL) v5.5 operating system (OS).

For detailed hardware platform and hard disk drive partition requirements, refer to the *Policy Provisioning Tool Overview* chapter of the *Policy Provisioning Tool Installation and Administration Guide*. For installation information, refer to the *Cisco MITG RHEL v5.5 OS Application Note*.

IMPORTANT

The Cisco MITG RHEL v5.5 OS is a custom image that contains only those software packages required to support compatible Cisco MITG external software applications. Users must not install any other applications on servers running the Cisco MITG v5.5 OS. For detailed software compatibility information, refer to the *Cisco MITG RHEL v5.5 OS Application Note.*

SCM Features in Release 12.0

This section provides information on new Session Control Manager (SCM) features in Release 12.0. Additional information on these features can be found in the *Cisco ASR 5000 Series Session Control Manager Administration Guide* and the *Cisco ASR 5000 Series Command Line Interface Reference*.

Advanced Congestion Control in CSCF Socket Layer

CSCF performs congestion control based on the memory usage inside every sessmgr at two levels.

Level 1: For every new call/event received, the system checks if sessmgr memory-usage is above a threshold value (such as 95 percent). If it is, memory-congestion is triggered and new call messages are rejected with 500 SIP response. Memory congestion is disabled when

memory usage drops by a tolerance value (default is 10 percent). This functionality has not been tested.

Level 2: If the sessmgr usage reaches 100 percent, all newly received SIP messages are dropped at the socket layer in that sessmgr except for the BYE message. The new SIP messages are not processed until the memory reaches the threshold value (95 percent).

A trap is also generated whenever sessmgr is in congestion state.

Bridge Mode: CSCF Session and Performance Counters Incremented for VoIP Calls.

When P-CSCF acts in a bridging mode between two services, the **`show cscf session counters calls`** *`<filter criteria>`* **`name`** *`<service_name>`* command now displays separate counters for access and core P-CSCF.

Cscfmgr Does Not Drop Register Requests for which Retries Exceeded When Congestion is Turned On in sessmgr

When cscfmgr (demuxmgr) receives REGISTER request from Network, it fetches a suitable sessmgr for processing REGISTER. If that sessmgr rejects the REGISTER since it is overloaded, cscfmgr will retry another sessmgr. If the system is congested, cscfmgr will retry three times to find a sessmgr. If it fails, then cscfmgr will reject the request with a “503 service unavailable” error response with Retry-after header.

CSCF Recovers All IMPUs Registered from Same Contact

CSCF now recovers all IMPUs registered from same contact.

CSCF Supports application/vnd.etsi.aoc+xml MIME Type

CSCF now supports application/vnd.etsi.aoc+xml MIME type as per spec TS 24.647 and proxies the message without parsing the message body.

CSCF Supports drop/reject/redirect Actions on Exceeding License Limits

The SCM now supports redirection on overload (exceeding session/license limit). Overload conditions arise when the maximum session limit per sessmgr is reached or the license is exceeded.

When the CSCF becomes overloaded, an overload policy can be configured to handle it. When the overload condition is hit, the new registrations (SIP REGISTER messages) reaching the cscfmgr are dropped/rejected/redirected based on the configuration.

CSCF Supports Multimedia Priority Service as per 3GPP TS 22.153

CSCF now supports multimedia priority service, as per 3GPP TS 22.153.

CSCF Supports “Retry-After” Header in 500 Response During Congestion

When CSCF identifies congestion, it originates UMM_RESPONSE with response code set as 500. Sipapp while forming the response SIP_IPS fills the Retry-after header with a random value between 0 to 10 seconds as per RFC 3261.

CSCF Supports RFC 5621 Message Body Handling in the Session Initiation Protocol (SIP)

CSCF has supported “multipart/mixed” message body parsing. It now also supports “multipart/alternative” and “multipart/related” message body parsing.

DSCP Marking

Provides support for more granular configuration of DSCP marking.

For Interactive Traffic class, the P-CSCF/A-BG supports per-service configurable DSCP marking for Uplink and Downlink direction based on Allocation/Retention Priority in addition to the current priorities.

I-CSCF Supports the Ma Reference Point for Interfacing to AS to Support Public Service Identity (PSI) Procedures

I-CSCF, upon receiving the terminating request, checks the subdomain-route list for matches. If a match is found the routing will happen based on it. Otherwise, I-CSCF will do a User Location Query (Location-Information-Request) and proceed normally.

P-CSCF Determines the Type of Authentication Based on the Rules in Annex P.3, 33.203 (860)

This functionality has been implemented, with the exception that NBA is not supported.

P-CSCF Provides Outbound Support with IPSec

P-CSCF now provides Outbound support with IPSec.

P-CSCF Rejects Emergency Calls Based on Local-policy/UE-location-network/SDP

P-CSCF will reject an emergency-call with 380 response based on the following local-policies (only if user is not emergency-registered):

- User is unregistered and makes an emergency-call (existing-option).
- User is non-emergency-registered and makes an emergency-call (existing-option).
- User is a visited-ue and makes an emergency-call. Here, visited-ue is determined based on matching of PANI in INVITE with MCC/MNC configured (new-option).

- User includes SDP with CS-Media in the INVITE of an emergency-call (new-option).

P-CSCF will reject an emergency-registration based on the following local-policies (new-options):

- Reject any new emergency-registration.
- Reject emergency-registration from a visited-ue. visited-ue is determined based on the existing functionality of PANI/default-aor-domain match.

P-CSCF Support for IPv6 with IPSec

Platform support for IPSec on IPv6 is available only on PSC2.

P-CSCF Support for Rx- 3gpp 29.214 v8.9.1

The following functions have been implemented in accordance with 3GPP 29.214 v8.8.0:

- Supported Features AVP:(Sec 5.6) is removed from RAR, RAA, ASR and ASA messages
- Supported Features AVP bit definitions have been modified (Sec 5.4.1)
- Flag definitions for Rx-reused AVPS have been changed (Sec 5.4)
- RAT change notification is now done along with IPCAN change notification (Sec 5.3.13,Sec 4.4.6.4)
- Specific Action AVP -CHARGING_ CORRELATION_EXCHANGE is now used for correlation exchange. Previously it was made obsolete.(Sec 4.4.6.5)
- STR send only after receiving AAA (Sec 4.4.4)

P-CSCF Supports Bridging and NAT functionality together

Added support for UEs from behind NAT in bridging setup.

P-CSCF Supports Interworking Between IPv4 UEs and an IPv6 IMS Core Network

P-CSCF now provides IPv4-IPv6 interworking functionality between IPv4-only UEs and IPv6-only core network elements (I/S-CSCF) by acting as dual-stack.

To achieve the dual-stack behavior, P-CSCF is configured in two services. The first service (V6-SVC) listens on an IPv6 address. The second service (V4-SVC) listens on an IPv4 address. SIP messages coming from IPv4 UEs will come to V4-SVC and be forwarded to the IPv6 core network through V6-SVC. Similarly, messages from IPv6 core network that come to V6-SVC can be forwarded to IPv4 UEs via V4-SVC.

P-CSCF Supports New IP-CANs

P-CSCF supports new IP-CANs, as per section 7.2A.5 of 24.229 (880).

P-CSCF Supports Special Handling for “Text” Media Type for Rx Interface

To meet regulatory requirements that deaf/hearing impaired people must be able to perform text-based communication to other users and government offices, the P-CSCF now supports Global Text Telephony.

Media type is set as “text” during media authorization with PCRF.

Global Text Telephony/Teletype messages must use ITU-T Recommendation T.140 for real-time text according to the rules and procedures specified in 3GPP TS 26.114 with the following clarifications:

- The UE must offer AVP for all media streams containing real-time text.
- For real-time text, RTCP reporting is turned off by setting the SDP bandwidth modifiers “RS” and “RR” to zero.
- Redundant transmission of real-time text characters is not to be used.
- The sampling time used is 300 ms.

PSC3 Hardware Support

The SCM supports the use of the Packet Service Card 3 in this release.

S-CSCF: Implemented an Internal Session-timer in B2BUA Mode

S-CSCF now runs a session timer in B2BUA mode for default of 1 hour.

S-CSCF Supports P-Served-User for SUBSCRIBE Requests

S-CSCF now supports P-Served-User for SUBSCRIBE requests.

Sequential Forking Functionality Working in B2BUA Mode

For a forking proxy server, the type of directive indicates whether the caller would like the proxy server to proxy the request to all known addresses at once (parallel), or go through them sequentially (serial) by contacting the next address only after it has received a non-2xx or non-6xx final response for the previous one.

Session Priority Support in Diameter RF interface

The Session-Priority AVP is now sent in Rf charging messages based on the SIP Resource-Priority header.

TLS Support in P-CSCF

Transport Layer Security (TLS) provides confidentiality and integrity protection for SIP signaling messages between the UE and P-CSCF/A-BG. TLS is a layered protocol that runs upon reliable transport protocols like TCP and SCTP.

The SCM supports the following two scenarios:

- TLS as a transport between UE and P-CSCF/A-BG, as per RFC 3261
- Use of TLS by Security Mechanism agreement between UE and P-CSCF/A-BG, as per RC 3329 and TS 33.203

SCM Features in Release 12.2

This section provides information on new Session Control Manager (SCM) features in Release 12.0. Additional information on these features can be found in the *Cisco ASR 5000 Series Session Control Manager Administration Guide* and the *Cisco ASR 5000 Series Command Line Interface Reference*.

AAA Required Only for 200 OK During Re-Invite

During Re-Invite, AAR is required to be sent only after 200 OK. Previously, it was also sent for INV message during re-invite procedure.

AAR Should Only be Sent for LTE Access

A new access-profile policy has been added for pcrf-control. This will enable pcrf-policy control to be enabled per access-type.

Unless the pcrf-policy-control is enabled for an access-type or in the default-access-profile, it will be disabled by default.

Active/Standby Groups for AS Routing

CLI has been added to support active/standby groups for AS Routing.

Add Configured Domain Based on Prefix in Request-URI

CLI **`route`** command, which specifies that a route lookup should be performed and the request URI modified, has been expanded to allow **`add`**, **`delete`**, and **`change`** options.

Added Support for “+g.oma.sip-im”

Added support for Accept contact feature tag “+g.oma.sip-im”.

AS Service-type Based Routing (Accept-contact)

During Registration, CSCF stores and manages the capability of UE. When a UE receives a call, the CSCF refers to the capability of that UE, and if the required service is not supported an error response is generated.

CLI has been added to configure UE capability failure to accept or reject with specific response code.

AS Triggering Based on Shared iFC

CLI added for displaying Initial Filter Criteria (iFC) in XML format, as per 3GPP TS 29.228 Annex E.

Authentication Flag in MAA Message

S-CSCF does not need to check subscriber's authentication if authentication flag is set to 0 in MAA message.

Block S-CSCF IP Going to UE in Service Route When Acting as A-BG

This functionality has been implemented.

Called-station-id AVP in AAR Removed

This functionality has been implemented.

Call Forwarding Failure

Call forwarding failed when History-info header from AS had syntax issue. Now, S-CSCF supports reserved type (blank, @) for History-Info value and forwards the INVITE with History-Info having reserved type (blank, @).

CSCF Handles Multiple Subscriptions in the Same Dialog

This functionality has been implemented in accordance with RFC 3265, 3.1.4.2.

CSCF Supports Multi-part ACL

Added support for multi-part ACL. Keywords can now be entered multiple times within a single command to support multi-part ACL in CSCF in the following CLI commands (CSCF ACL Configuration Mode):

- deny
- permit
- redirect

CSCF Supports REGI Management

- Display of Registration timestamp in **`show sub cscf-only full`** CLI output
- Do not validate authorization received from UE for challenge re-register
- Skip SAR for Re-Registration
- Reply 200 OK for Re-Register in case of HSS Failure.

Custom AVP in ACR

When new CLI is enabled, User Name AVP will be filled with Public User ID with URI Scheme in ACR message.

Custom Feature Tags Supported

CLI has been added to use custom tags to represent UE capabilities.

Custom Registration Binding

CLI command added to enable the S-CSCF to return only one binding (latest contact) for each registration without including other bindings, if any.

Diameter Support for CDF Prefix Based Routing

Diameter updated to support CDF prefix/capability based routing.

Different RCS-e Tags Need to be Processed Separately

Previously, all RCS-e tags were processed as the same tag. Now, they are processed separately and Rf feature-code AVP is sent accordingly.

Disable IPSec Based on CLI Option

An extra parameter has been added to the existing CLI to insert integrity-param in P-CSCF.

Disable UAR/UAA: P-CSCF to select the S-CSCF based on destination routing or DNS routing

If new **`user-authorization`** CLI command is enabled, and I-CSCF role is enabled in S-CSCF, I-CSCF will send UAR/UAA diameter message to HSS.

Diversion Header Customized and Support for Additional Rf AVPs

Custom Diversion header supported.

The following new Rf AVPs are also now supported:

- RF-LGUPLUS-Start-Time
- RF-LGUPLUS-End-Time
- RF-LGUPLUS-Service-Type
- Recipient-Code
- Call-Integrity
- AIN-Indicator
- Call-Forwarded-Address

DNS Lookup Table Entries Increased to 1024

The maximum number of entries for **`ip localhost`** CLI command has been increased from 256 to 1024.

Domain Name in OPTION Message

When **`custom volte`** command is enabled and hostname is configured, S-CSCF will add hostname:service-port in From header of OPTIONS request.

Feature Parameter in the ACR for Feature Code

Feature parameter in the ACR must include the feature code based on the P-LGTVTS-Charging-Data.

Forking Based on CLI

New CLI controls the default-request forking-type in S-CSCF.

Forking Based on the P_xxx_forking_list Header

Added changes to support Forkidlist and device id.

Handling FQDN for CDF Address When “custom volte” Enabled

Previous Behavior

The CDF address provided by HSS is used when no CDF matches the “prefix and capability based selection criteria”, then:

1. The CDF address provided by HSS is handled as plain CDF address itself.
2. CSCF supports handling of more than one CDF address, such as primary and secondary CDF.

This was the default behavior.

New Behavior

The CDF address provided by HSS is used when no CDF matches the “prefix and capability based selection criteria”, then:

1. The CDF address received from HSS will always be treated as a AAAGroup Name. The FQDN/IP and port part of address will be extracted and used as AAAGroup name.
2. CSCF will only support one CDF address.

This is now the default behavior.

HSS Prefix Based Selection for LIR/LIA

HSS prefix based selection for LIR/LIA supported.

The keyword **source** has been removed from the following command in the *CSCF Diameter Selection Configuration Mode*.

Previous:

[no] aaa-group *name* **criteria { source aor** *aor_prefix* **| subscriber-capability { audio [only] | text | video } | subscriber-ip-type { v4 | v6 } } +**

Now:

[no] aaa-group *name* **criteria { aor** *aor_prefix* **| subscriber-capability { audio [only] | text | video } | subscriber-ip-type { v4 | v6 } } +**

Previously, if **criteria source aor <***aor-prefix***>** was configured, fetching of aaa group name was done based on source aor. Now, fetching of aaa group name for a subscriber can be based on source aor match or destination aor match.

HSS Prefix Based Selection Over Cx Interface

This functionality has been implemented.

HSS Selection CLI Modified for Easy Updating

To support re-arrangement of prefix related configuration, preference will be associated with each diameter selection entry in the diameter selection table. The keyword **preference** and its options have been added to the **aaa-group** command in CSCF Diameter Selection Configuration Mode.

If preference is specified, the entry matching the preference is updated.

If preference is not specified, it is assigned a preference one greater than the last entry's preference in the diameter selection table.

Preference is mandatory for diameter selection entry deletion.

The preference associated with each CLI is displayed in show configuration output.

HSS Selection Method

New CLI configures matching criteria for selecting a AAA group name. When a subscriber registers, the selection criteria are compared and the AAA group name from the matching entry will be picked up. The selected AAA group will be used for all HSS interactions for that subscriber. Maximum of 3 criteria can be configured per entry. A maximum of 1024 such entries can be configured.

HSS selection need not be done for Re-Register.

I-CSCF Added Functionality

The following features have been implemented for the I-CSCF in this build:

- Ability to retry Register on a second S-CSCF server based on UAR returned capabilities when the first server times out or sends an error response
- Congestion control
- License management

ICSR Support for IMS

ICSR is supported for the following:

- Basic registration
- Basic call
- Subscribe/Notify
- Diameter information for Rx
- CSCF session-related counters
- GRUU
- Subscriber statistics

Implicit Expires Timer Configured for REGISTER

New CLI specifies the implicit amount of time that a registration can exist on the system.

If the implicit timer is configured and the UE time expires, then the system responds with 200OK with Expires-header set to configured implicit-expires time.

If implicit timer is not configured, then previous logic of sending 423 response is used.

INVITE Message to AS Modified

When **`custom volte`** command is enabled, “TYPE 3” tag in the IOI is not sent to AS. S-CSCF adds orig-ioi parameter in P-Charging-Vector while sending towards AS in all SIP method scenarios (except REG).

Unwanted AVPs are also removed from custom Rx dictionary.

Monitor Protocol Support for RTP packets

The following two protocols have been added to the system's protocol monitoring utility initiated by the **`monitor protocol`** CLI command:

- RTP (IMS)
- RTCP (IMS)

Multi-domain Support

User may register with a domain other than the default-aor-domain.

New AVPs for AAR Added

For invite, the following new AVPs have been added in AAR message:

- AF_Applicatoin _Id
- calling party address
- called party address
- ROLE of Node

New Rf-Interface AVPs Supported

New diameter authentication custom dictionary "aaa-custom5" added for Rf interface to support the following new AVPs:

- Service-type
- Call-Forwarded-Address
- Recipient-Code
- Call-Integrity
- AIN-Indicator
- Feature-Code

New Rx-Interface AVPs Supported

New custom dictionary "rx-custom01" added for Rx interface to support the following new AVPs:

- AF_Applicatoin _Id
- calling party address
- called party address
- ROLE of Node

Additional custom dictionary name changes made in Proxy-CSCF Configuration Mode.

NPDB Support Using Multiple Client IP Addresses

Multiple **`bind`** commands now supported for each NPDB client in CSCF NPDB Client Configuration Mode.

Number of SiFC-IDs per Subscriber in Received SAA can be More Than 20

Previously, S-CSCF could only support a maximum of 20 SiFC IDs per subscriber.

Now, 48 SiFC-IDs are supported per subscriber.

Outbound ACL Support for Handling Terminating Domain

New aclLookUp APIs added in standalone request states in callLeg.

P-CSCF Adds Rport Param in Hosted NAT Scenarios

P-CSCF now adds rport param in hosted NAT scenarios.

P-CSCF Removes the P-LGUPlus-PRID Header Towards UE

P-CSCF removes the P-LGUPlus-PRID header received from S-CSCF while forwarding to UE.

P-CSCF Supports Redirection of UE

- CSCF applies new inbound-acl criteria on incoming requests.
- New option added to redirect the request to other CSCFs.
- New parameter added to existing options to check ACL criteria for subscriber capabilities.

P-CSCF Supports P-Profile-Key header

If the identity of the served user of the request was taken from the P-Preferred-Identity header field by its matching a registered wildcarded public user identity and the P-CSCF supports the SIP P-Profile-Key private header extension, The P-CSCF now includes the wildcarded public user identity value in the P-Profile-Key header field, as defined in RFC 5002.

P-LGUPlus-PRID-Info Added in All Out-of-dialog Requests

New CLI allows a custom specific header, P-LGUPlus-PRID-Info, which contains the private user id of the user sending any dialogue crating request or any standalone requests, to be added in the message toward nexthop. The addition of this custom header will be done when Proxy-CSCF forwards this message.

Port Range Configuration Supported for Media Bridging

New keyword **`v6port-range`** in **`media-bridging`** CLI command specifies port ranges to be used with IPv6 addresses. Only selected ports from the range specified should be used for media bridging.

PRID Shown in subscriber cscf-only full Command Output

Private User ID is now shown in output of CLI command **`show subscribers cscf-only full`**.

Redirection Based on User-Agent Header Supported

CLI has been added to support redirection based on User-Agent Header.

Registration of Multiple Devices with Different device-type

Registration of multiple devices with different device-type for same private userid.

Routing Control Depending on Terminal Capability Registered

CLI has been added to configure UE capability failure to accept or reject with specific response code.

SBC Media Loss Detection Timer Made Configurable

New keyword **`timeout`** in **`release-call-on-media-loss`** CLI command specifies the media loss timeout value; media loss after timeout value results in call release.

S-CSCF Able to Send Dummy-AS 200OK Response

If the AS which is triggered by iFC has a problem, new CLI allows configuration of the reply value for that peer AS.

S-CSCF Adds GRUU Towards AS in P-LGUPlus-Instance-Info Header

Fulfilled requirement to add P-LGUPlus-Instance-Info header with value of Public-GRUU generated by S-CSCF towards AS.

S-CSCF Not Sending Message to P-CSCF After Receiving 603, 486, 415 from AS

AS changes tag in To header for these messages. Now, S-CSCF forwards 183 responses with different To-tag.

S-CSCF Sends P-LGUPlus-PRID-Info in REGISTER Message Sent Toward AS

New CLI allows a custom specific header, P-LGUPlus-PRID-Info, which contains the private user id of the user sending the REGISTER request, to be added in the REGISTER message towards AS during third party registration.

S-CSCF Subdomain Based PSI Routing

When the Request URI in the incoming request matches the locally configured PSI, then I-CSCF must not do location query and must route the request based on the internal DNS.

S-CSCF Support for IPv6 to IPv4 Interworking

The following interworking scenarios have been addressed in this release:

- Handling 3xx responses containing Contacts with different IP versions
- Follow-me URIs with different IP versions
- Multiple peer-servers with different IP versions using hunting logic

S-CSCF Supports P-Profile-Key header

When the S-CSCF does not have the user profile, it initiates the S-CSCF Registration/Deregistration notification procedure, as described in 3GPP TS 29.228; with the purpose of downloading the relevant user profile and informs the HSS that the user is unregistered.

The S-CSCF will assess triggering of services for the unregistered user, as described in 3GPP TS 29.228. When requesting the user profile the S-CSCF can include the information in the P-Profile-Key header field in the S-CSCF Registration/deregistration notification.

Selective Interworking with Multiple MGCFs and MGCF

New criteria added when choosing routing criteria for the CSCF service.

Selective Interworking on AS Capability and Subscriber Prefix

New criteria added when choosing routing criteria for the CSCF service.

Separation of traffic to/from BGCF

SCM now supports the separation of traffic to/from BGCF.

Server Name AVP in MAR and SAR

CLI command added to enable the S-CSCF to fill the server name AVP in MAR and SAR for Cx interface with configured server name.

Session Released when RAR with Event 4 is Sent by PCRF

Session is released when RAR with event INDICATION_OF_RELEASE_BEARER (4) is received from PCRF.

Shared IPv6 Prefix Used for v4v6 Interworking

Instead of using a different IPv6 prefix for each subscriber, using shared-prefix pool at VPN level. With this, first 64 bits remains the same for all the users across different session managers.

SiFC Not Triggered When SiFC Set ID Received Without Extension

This functionality has been implemented, as per 3GPP TS 29.228.

SiFC ID Number Configuration in CLI Increased

SiFC ID number configuration in CLI increased to 1 - 2,000.

The system now stores 1,000 SiFC IDs per context; previously, it was 256.

Support Enable/Disable of AAR for 18X Response

CLI has been added to support enabling AAR for 180, 183 and 18X responses. If disabled, then AAR will not be sent when system gets 18X from AS or other peers.

Support for Displaying of Connection Status to NPDB Server

NPDB connection status shown using CLI.

Support for Custom AVPs for MAR/MAA Over Cx Interface

New diameter authentication custom dictionary “aaa-custom8” added.

Support for Custom AVPs in MAR Over Cx

The following AVPs need to be filled in MAR message before sending it on Cx Interface:

- SIP-Authentication-Context
- SIP-AOR
- User-Agent

Support for Custom NPDB

CLI has been added to support the NPDB (Number Portability Data Base) feature. NPDB is based on a client server architecture. NPDB client in S-CSCF service performs query for called subscriber number on NPDB server, which returns Routing Number for the query.

NPDB client uses TCP connection to the NPDB server through the sessmgr and maintain a prefix table with 1,000 entries.

Support for HSS/CDF Server when RF CEA Does Not Have Acc-App-Id

Previously, CER/CEA received without Acct-Application-Id AVP was considered an error.

Now, CER/CEA messages received without Acct-Application-Id are not considered an error for customer-specific Rf.

Support for HTTP-Digest-MD5 custom auth-algorithm

New CLI allows a **`custom-md5`** option in authentication configuration.

Support for LIA Based Routing Using MS Status

LIA based on the MS Status from the LIA message. The system can route, accept, or reject-with-error-code the call based on MS Status code from LIA message.

Support for LIR Media-Type and P-LGT-Term-Status

LIR now fills the Media-Type AVP.

MS-Status-AVP data is now also copied into P-LGT-Term-Status SIP header, which is added by I-CSCF and sent to terminating S-CSCF. Terminating Application server uses this P-LGT-Term-Status SIP header to execute the supplementary features.

Support for Prefix/Capability Based CDF Selection

New CLI is added for enabling or disabling CDF selection per access-type.

Support for TPS Based Control Towards AS

New CLI added to control the rate of messages going from S-CSCF to application server (AS) based on Transactions Per Second (TPS).

Support for Triggering NOTIFY Through reg-event

New CLI enables reg-event package at S-CSCF. System will send 501 “Not implemented” if the CLI is not enabled.

Support PCRF Interworking with Options to Reject/Proceed Call

This support is only for INVITE. If PCRF is enabled and PCRF server is down, REGISTER is expected to fail.

Support Showing of IPv4/v6 Subscribers

CLI command **`show subscribers`** enhanced.

System Must Provide Session Management

Session query based on the subscriber number now includes session category (type), starting time, and calling/called number.

Tel-URI to SIP-URI Conversion

CLI has been added to support converting a Tel-URI to SIP-URI.

Timer C Made Configurable

CLI has been added to support configuration of Timer C.

ue-capability-failure - Custom Response Codes Configurable per RCS-e Tag

Previously, all RCS-e feature tags uses a single ue-capability-failure response code. CLI has been added in route selection, hss selection, ue-capability-failure response code, and ACL configuration to support configuring response codes for each RCS-e feature tag.

Update Calling-Party AVP in CDR with Diversion-Header for Call-Forward

If a call is forwarded by AS and the Diversion header is included in INVITE, the header value is used as calling party of CDR.

Updated “Service-Info-Status” AVP in AAR to Indicate 18x or 200

CSCF has added a new indication in AAR message for 18X or 200OK.

3GPP “Service-Info-Status” AVP includes a new value “2” (PROVISIONAL_RESP_INDICATION_SERVICE_INFORMATION(2)) in custom dictionary rx-custom01. This indicates that the AAR was triggered for 18x response.

V Bit Should be Set for Called-party-address AVP in AAR

V bit is now set for Called-party-address AVP.

All PCRF using Rx interface should support this.

Via Header Type Customer Requirements

S-CSCF will always use IP address in Via header, regardless of bind address hostname.

P-CSCF will use IP address towards network and hostname towards UE if configured.

Serving Gateway Features in Release 12.0

This section provides information on new Serving Gateway (S-GW) features in Release 12.0. Additional information on these features can be found in the *Cisco ASR 5000 Series Serving Gateway Administration Guide*.

Circuit Switched Fallback Support

Circuit Switched Fall Back (CSFB) enables the UE to camp on an EUTRAN cell and originate or terminate voice calls through a forced switchover to the CS domain or other CS-domain services (e.g., Location Services (LCS) or supplementary services). Additionally, SMS delivery via the CS core network is realized without CSFB. Since LTE EPC networks were not meant to directly anchor CS connections, when any CS voice services are initiated, any PS based data activities on the EUTRAN network will be temporarily suspended (either the data transfer is suspended or the packet switched connection is handed over to the 2G/3G network).

While the primary responsibility of supporting CSFB fall to the MME, the S-GW supports CSFB messaging over the S11 interface.

IKEv2 IP Security Support on S1-U and S5 Interfaces

IP Security (IPSec) on the S1-U and S5 interfaces is a node-to-node IKEv2 tunnel that can be configured to assume the characteristics of either a pre-configured tunnel or a dynamic tunnel.

Pre-configured node tunnels are fully qualified IPSec tunnels. Each IPSec tunnel is configured with parameters including pre-shared key, local and remote IP addresses, crypto hashes, groups, algorithms and the access control list (ACL).

Node-to-node dynamic tunnels are generated dynamically as the connections are initiated by different nodes in the LTE network. Each IPSec tunnel does not need to be pre-configured for each required parameter, instead it uses a common template for some parameters, like crypto algorithms, hashes, and groups. Other parameters are fetched dynamically from the tunnel requests like IP addresses and traffic selectors. Authentication information is fetched dynamically via certificates.

Typically, the eNodeB initiates an IPSec tunnel to the S-GW. The S-GW service is responsible to verify the configuration and use an IPSec API to make the S-GW listen on the service address for IKE requests.

When configured for IPSec, the S1-U interface carries subscriber data traffic and the S5 interface carries GTP-C signaling traffic and GTP-U data traffic that flows through an IPSec tunnel.

Multiple PDN CDR Information Transmission Behavior Change

Previous Behavior: Upon receiving RAT type, ULI, and MS timezone information from the MME for an additional PDN in a multi-PDN call, the S-GW would send this information on to the P-GW even if theses parameters had not changed. Also, if these parameters were only for one of the PDNs in a multi-PDN call, they were reported as the parameters for all the PDNs.

New Behavior: The S-GW now forwards RAT type, ULI, and MS timezone only if there are changes to these parameters. If these parameters are only reported for one PDN in a multi-PDN call, they are only identified for the PDN for which they belong in the CDR.

Operator Policy

The operator policy provides mechanisms to fine tune the behavior of subsets of subscribers above and beyond the behaviors described in the user profile. It also can be used to control the behavior of visiting subscribers in roaming scenarios, enforcing roaming agreements and providing a measure of local protection against foreign subscribers.

X.509 Certificate-based Peer Authentication

The S-GW supports X.509 certificate-based peer authentication for IPSec tunnels.

Serving Gateway Features in Release 12.2

This section provides information on new Serving Gateway (S-GW) features in Release 12.2. Additional information on these features can be found in the *Cisco ASR 5000 Series Serving Gateway Administration Guide*.

CSFB Support

The S-GW now forwards Suspend/Resume messages towards the P-GW as an enhancement to the Circuit Switched Fallback (CSFB) feature in compliance with 3GPP Release 9.

The S-GW forwards Suspend Notification messages towards the P-GW to suspend downlink data for non-GBR traffic; the P-GW then drops all downlink packets. Later, when the UE finishes with CS services and moves back to E-UTRAN, the MME sends a Resume Notification message to the S-GW which forwards the message to the P-GW. The downlink data traffic then resumes.

Downlink Data Notification Delay Timer

A new configuration command is available to help calculate a timer that delays the sending of excess Downlink Data Notification messages by the S-GW to the MME in instances where downlink data is received before a Modify Bearer Request.

Emergency Session Support

The S-GW now supports Emergency PDN handling based on 3GPP Release 9.

GTP-U Sequence Number

CLI command added to enable/disable addition of the sequence number to every GTP-U packet coming from Gi interface and going towards Gn/Gp interface. If GTP-U packets are received out of sequence, sequence numbers would allow the packets to be reordered.

Lawful Intercept

TCP Proxy Support

TCP Proxy support is now available for Lawful Intercept on the S-GW. Contact your local sales representative for detailed information.

Notification of LI Target Modification/Deletion

The S-GW now supports the sending of a notification to LI administrators when an existing LI target provision has been modified or deleted. Contact your local sales representative for detailed information.

Location Reporting

Location reporting can be used to support a variety of applications including emergency calls, lawful intercept, and charging. This feature reports both user location information (ULI) and user CSG information (UCI).

- ULI data reported in GTPv2 messages includes:
- TAI-ID: Tracking Area Identity
- MCC: MNC: Mobile Country Code, Mobile Network Code
- TAC: Tracking Area Code

UCI data reported in GTPv2 messages includes:

- MCC: MNC: Mobile Country Code, Mobile Network Code
- CSG-ID: Closed Subscriber Group Identifier
- Access Mode: CSG access mode received from the source eNodeB or RNC

The S-GW stores the ULI and UCI, and also reports the information to the accounting framework. This may lead to generation of Gz and Rf Interim records. The S-GW also forwards the received ULI and UCI to the P-GW. If the S-GW receives the UE time zone IE from the MME, it forwards this IE towards the P-GW across the S5/S8 interface.

Additionally, if the S-GW receives the UE timezone from S11/S4 interface, it now forwards this information to the P-GW.

Rf/Gz Accounting Support Using Operator Policy

The Diameter Rf interface supports offline charging (3GPP 32.240) for network services that are paid for periodically. For example, a user may have a subscription for voice calls that is paid monthly. The Rf protocol allows an IMS Charging Trigger Function (CTF) to issue offline charging events to a Charging Data Function (CDF). The charging events can either be one-time events or may be session-based.

The S-GW supports the enabling of this Diameter interface via operator policy. Options for accounting mode include: GTPP (default), RADIUS / Diameter or None.

SGSN Features in Release 12.0

This section provides information on new Serving GPRS Support Node (SGSN) features in Release 12.0. Additional information on these features can be found in the SGSN Release Notes available with the new releases, in the *SGSN Administration Guide*, and in the *Command Line Interface Reference*.

Max Number of LACs Configurable for Gs Service Increased

The configuration limits have increased from 32 to 128 for the maximum number of LACs, as a combined total for LACs configured, for pool-areas and non-pool-areas for a Gs Service.

Max Number of LACs / Zone Code List - Behavioral Change

Maximum number of LACs per allowed zone code list has increased from 10 to 100.

2G Attach Failure Statistics Enhanced

The software has been modified to more accurately segregate and represent 2G attach failure rates due to internal errors vs. procedure collisions. Multiple counters have been added, and some modified, to peg specific failures due to internal errors, and to peg failures due to ongoing procedure collisions, and counters added to log total attach failures due to internal errors.

The purpose and meaning of the ‘total-attach-failure’ counter has changed from being a combination of attach failures due to ongoing procedures and internal errors. Now the counter represents attach failures due only to internal errors.

2G Detach Request Sent To MS - Behavioral Change

Previous Behavior: During a 2G call, when Cancel Location was received after Attach Accept is sent, the SGSN was not sending Detach Request.

New behavior: Now during a 2G call, if a Cancel Location is received after Attach Accept is sent, then Page Request will be sent and after page Response, Detach Request will be sent to the MS. If Attach Accept has not been sent, the Attach Reject will be sent.

2G-PS-Page-Responses Statistics - Behavioral Change

Previous Behavior: The page response statistics are not pegged on receiving cell-update in response to paging.

New Behavior: The page response statistics are pegged on receiving cell-update in response to paging.

Impact on customer: The paging-success rate is improved.

3GPP 23.008 Regional Subscription Information (RSZI)

The SGSN now fully supports regional subscription zone identities (RSZIs) in accordance with TS 23.008. The HLR stores a list of RSZIs; 10 per network destination code (NDC). The RSZI are comprised of the PLMN id and the zone code lists. The SGSN now enables the operator to define the zone code lists, to enable zone code checking, and to define the cause code for subscription rejection when it is due to regional subscription information failure.

3G NRPCA

The SGSN now supports the Network Requested PDP Context Activation (NRPCA) procedure for 3G attachments. Whenever there is downlink data at the GGSN for a subscriber, but there is no valid context for the already-established PDP address, the GGSN initiates an NRPCA procedure towards the SGSN. Prior to starting the NRPCA procedure, the GGSN either obtains the SGSN address from the HLR or uses the last SGSN address of the subscriber available at the GGSN. There are no interface changes to support this feature. Support is configured with existing CLI commands (network-initiated-pdp-activation, location-area-list) in the call-control-profile configuration mode and timers (T3385-timeout and max-actv-retransmission) are set in the SGSN service configuration mode.

APN Remapping Based on Charging Characteristics - Behavioral Change

Previous Behavior: The original APN remapping behavior was such that if any of the subscription record had matching charging characteristics then the requested APN would be remapped to the configured APN <*apn_net_id*>.

New Behavior: APN remapping behavior has been modified so that remapping occurs only when the charging characteristics value in the subscription record associated with the requested APN matches the configured value. This will avoid remapping of all APNs that the subscriber requests. This change is implemented with the new **new-ni** keyword of the **cc** command in the APN Remap Table configuration mode - explained in “Modified Commands” section of the *Configuration Management* chapter.

APN custom33 Encoding of S-CDRs - Behavioral Change

Previous Behavior: In the custom33 dictionary, the APN OI and NI were length encoded.

New Behavior: In the custom33 dictionary, the APN OI and NI are dot encoded.

APN Handling / Default APN - Enhanced

For a PDP context request, an invalid APN occurs when none of the APNs in the HLR subscriber profile match the APN sent by the subscriber. The SGSN can now be provisioned to override an invalid APN even when a user has a wildcard APN in the HLR profile. The SGSN’s existing default APN functionality has been enhanced so that if a required subscription APN is not present in the subscriber profile, then the SGSN will now continue the activation with another configured 'dummy' APN. The call will be redirected, via the GGSN, to a Webpage informing the user of the error and prompting to subscribe for services.

Previously, if the required subscription APN was not present in subscriber profile, activation would be rejected.

APN Override Enhancements

The SGSN now provides the ability to configure default APN to be used in several different scenarios:

• Use the APN in the first subscription record as a default APN. With this option the first subscription record with matching PDP type and PDP address will be used as the default APN. Here, first record means the first among the records received from HLR in that order. The default APN will be used if normal APN selection fails. This function is enabled via the new key-word ‘**first-in-subscription**’.

• Fallback to the APN in the first subscription record when configured default APN is not available. It is possible to configure a default APN to be used. However, if the configured default APN is not present in subscription then the SGSN will use the APN in the first

subscription record with matching PDP type and PDP address. This function is enabled via the new keyword '**fallback-to-first-in-subscription**'.

• Prefer to use a single subscription record option, which specifies that if normal APN selection fails and if there is only one subscription record, then use the APN in that subscription record as the default APN. This is an optional configuration and is specified along with a default APN to be used. The configured default APN will be used when there are more than one subscription records. This feature is enabled via the new keyword '**prefer-single-subscription**'.

APN Profile and IMEI Range Associations - Behavioral Change

Previous Behavior: The maximum number of APN profiles that could be associated with an operator policy was 50. The maximum number of IMEI ranges that could be associated with an operator policy was 10.

New Behavior: The maximum number of APN profiles that can be associated with an operator policy has increased from 50 to 128. The maximum number of IMEI ranges that can be associated with an operator policy has increased from 10 to 128 IMEI ranges.

APN Resolution with SCHAR and Optionally RNC-ID

It is now possible to append subscriber charging characteristic (SCHAR) information to the DNS string. The SGSN includes the profile index value portion of the CC as binary/decimal/hexadecimal digits (type based on the configuration) after the APN network identification. The charging characteristic value is taken from the subscription record selected for the subscriber during APN selection. This enables the SGSN to select a GGSN based on the charging characteristics information.

After appending the charging characteristic the DNS string will take the following form: **<apn_network_id>.<profile_index>.<apn_operator_id >**. The profile index in the following example has a value 10: **quicknet.com.uk.1010.mnc234.mcc027.gprs**.

If the RNC_ID information is configured to be a part of the APN name, and if inclusion of the profile index of the charging characteristics information is enabled (per this enhancement) before the DNS query is sent, then the profile index is included after the included RNC_ID and the DNS APN name will appear in the following form: **<apn_network_id>.<rnc_id>.<profile_index>.<apn_op erator_id>**. In the following example, the DNS query for a subscriber using RNC 0321 with the profile index of value 8 would appear as: **quicknet.com.uk.0321.1000.mnc234.mcc027.gprs**.

APN Selection of GGSN/PGW based on Network Capability - Behavioral Change - Demo Support

Previous Behavior: The SGSN could only select a GGSN (perform only DNS "A" queries).

New Behavior: The SGSN can also perform a DNS "SNAPTR" type (Straightforward Name Authority Pointer) query to select a PGW if the mobile UE is Release 9 compliant.

The Gn/Gp SGSN can now be configured to select a combined PGW/GGSN node to anchor a PDP context. During PDP context activation, after the APN is selected, normally a Gn/Gp SGSN does a DNS A/AAA query to resolve the APN into a GGSN IP address. Now, if the MS and the network are both EPC-capable, then the Gn/Gp SGSN should select a combined PGW/GGSN node to anchor the PDP context. This will enable the subscriber to roam into an EPC network without losing the PDP context.

In order to support PGW selection for an MS that is EPC capable, an SGSN shall do a DNS SNAPTR query for APN resolution.

If this feature is not enabled on the SGSN, the SGSN proceeds with the selection of a GGSN as usual, despite the UE ‘s network capability. Without this feature, whenever a release 9 compliant UE moves from a 2G/3G network to a 4G network, the PDP context has to be deactivated from the GGSN and a new activation towards a PGW is needed.

With this feature enabled, the signaling load on the network side is reduced because the deactivation and activation procedure is avoided when the SGSN selects a PGW during 2G/3G activation.

Avoiding PDP Context Deactivations - Behavioral Change

Default behavior has been changed to avoid PDP context deactivations resulting from GTP-C path failure detection due to messages containing erroneous restart counter change values.

Previous Behavior: The old default behavior was to have the SGSN detect GTP-C path failure based upon receiving restart counter changes in messages (Create PDP Context Response or Update PDP Context Response or Update PDP Context Request) from the GGSN and immediately begin PDP deactivation with a reactivation message. If the values in the messages are spurious, then this behavior could result in undesirable increases in network traffic due to bursts of deactivations/activations.

Bulk Stats for Simple and Combined Attach Failures

Previous Behavior: The SGSN code does not provide counters or bulk statistics that support segregation of internal and external triggers for 2G Attach Failures.

In the CLI output the following counters account only for internal triggers (Internal Errors) for 2G Attach Failures:

- 2G-Attach-Failure
- Gprs-Attach-Failure
- Comb-Attach-Failure

The following bulk statistics account only for internal triggers (Internal Errors) in 2G Attach Failures:

- 2G-total-attach-fail
- 2G-total-attach-fail-comb

- 2G-total-attach-fail-all

New Behavior: The SGSN code has been modified to segregate for both internal and external errors enabling the following CLI counters to account for both internal and external triggers for Attach Failures:

- 2G-Attach-Failure
- Gprs-Attach-Failure
- Comb-Attach-Failure

The following counters in bulk statistics account for both internal and external triggers for Attach Failures:

- 2G-total-attach-fail
- 2G-total-attach-fail-comb
- 2G-total-attach-fail-all

Impact on customer: The values of the above mentioned counters increase due to the change in behavior. A drop in the counter “2G-attach success rate” is observed if the same counters are used for calculating KPIs.

Bulk Stats New for Iu Release before 3G Attach

Previous Behavior: There was no break up in the SGSN code to separately indicate internal and external triggers that lead to Iu being released before Attach in 3G.

New Behavior: New CLI counters and new bulk statistics have been added to support the segregation of internal and external triggers for Iu being released when it occurs prior to a 3G Attach. With the new counters, the operator has the flexibility to choose either internal or external triggers to compute KPIs.

Bulk Stats Track 2G Attach Rej with Network Failure Cause Code

Previous Behavior: Prior to this release, the SGSN counters did not support segregation of internal and external triggers that lead to 2G Attach Reject with a “Network Failure” cause code.

New Behavior: With this release, new bulk statistics are added to indicate both internal and external triggers that lead to 2G Attach Reject with a “Network Failure” cause code. With the new counters, the operator has the flexibility to choose either internal or external triggers to compute KPIs.

IMPORTANT

Currently, the internal failure triggers for 2G Attach Reject with “Network Failure” cause code are not available.

Bulk Stats Track 3G Attach Rej with Network Failure Cause Code

Previous Behavior: The existing SGSN counters do not support segregation of internal and external triggers that lead to 3G Attach Reject with “Network Failure” cause code.

New Behavior: New counters are added to indicate internal and external triggers that lead to 3G Attach Reject with “Network Failure” cause code. With the new counters, the operator has the flexibility to choose either internal or external triggers to compute KPIs.

CLI Override to Inform RNC before UE of QoS Change

Previous Behavior: When there is a change in QoS, due to inter-RAT handover from 2G to 3G or inter-SGSN handover and with no RAB being established during handover, followed by downlink data or service request of type data, the SGSN first informed the UE of the new QoS through a “Modify PDP Context Request” and later setup the RAB.

New Behavior: The new CLI “qos-modification” has been added to the SGSN Service configuration mode to enable the operator to override the SGSN behavior. With this override, the SGSN will inform the RNC of new QoS before informing the UE during downlink data procedures and service request for data procedures. SGSN will setup the RAB first, followed by either sending “UPCQ” towards the GGSN OR by sending “Modify PDP Context Request” towards the UE, depending on whether or not the RNC downgrades the QoS.

Impact on Customer: With this CLI control override enabled, the call flow during downlink data or service request of type data will be different

Ciphering Algorithm Negotiation Failure - Actions Configurable - Behavioral Change

Previously, if there was no match between the ciphering algorithm from the MS and the ciphering algorithm configured in either the call control profile or the GPRS service configuration, then the SGSN performed Attach or RAU without ciphering.

Now, the SGSN can be configured to either:

- Allow the call without ciphering (geo0)
- Reject an incoming Attach / RAU when there is not a match between the MS and SGSN configured ciphering algorithms. The call Attach/RAU Rejection message can include a configurable GMM failure code.

Configurable SCTP Receiver Window Size - Behavior Change

It is now possible for the operator to configure a reduced priority for Link Manager Control messages, thereby giving timer messages the highest priority. The timer messages are retained at the highest priority and data messages are kept at a lower priority. As a part of this enhancement, a new parameter, **`sctp-init-rwnd`**, will enable the SCTP association to maintain a configurable window at the receiving end.

Configurable Start for MS Authentication on First Vector

To avoid high traffic levels during PDP establishment, the SGSN has been modified to reduce the attach time, as much as possible, so that the devices can attach and discontinue sending requests. This change is intended to reduce the time needed to retrieve vectors over the Gr interface by allowing the operator to configure the SGSN to start authentication towards the MS as soon as it receives the first vector from the AuC/HLR. With the change to the configuration, the SGSN begins the MS authentication process immediately after receiving the first vector from the HLR, while the SAI continues in parallel.

Continue with Attach when EIR is Unreachable

The attach process may continue in the case of an IMEI check timeout, based on the SGSN service and/or the GPRS service configuration. But the attach only proceeds if the route towards the EIR is up and the IMEI request timer expires.

The software has been enhanced to configure the SGSN to allow the attach process to continue if the route towards the EIR is down, e.g., the DPC / SSN is out of service. This new CLI control command has been added to SGSN service and GPRS service configuration modes.

Controlling THP and ARP via Operator Policy

The SGSN's local QoS THP and ARP configurations can now override the QoS traffic handling priority (THP) value and allocation/retention priority (ARP) from an HLR subscription. This QoS capping can be done on a per-APN basis and is configurable in the APN profile for use through the operator policy function.

This functionality can differentiate home vs. roaming subscribers, and prevent visiting subscribers from receiving a high-tiered service. For example, a service provider could offer service differentiation using Ultra/Super/Standard service levels based upon QoS; this could justify charging a corporate customer more to use the Internet APN than would be charged to a consumer. This could be accomplished by controlling the traffic handling priority (THP) over the air interface, i.e. THP 1 = Ultra, THP 2 = Super and THP 3 = Standard. But this must be configured at the operator policy level to prevent a "roamed-in" customer from getting Ultra service if the foreign subscriber's network provisions all of their customers with THP 1 on their HLRs.

Commands and Counters Added To Display 2G And Combined Attach Reject Scenario Reasons

Different internal or external triggers/reasons lead to 2G Attach Reject scenarios. 2G Attach Requests are rejected with network failure cause codes. New counters are added to indicate each of the different kinds of triggers. The operator is provided the flexibility to configure the display of triggers.

Commands and Counters Added To Display 3G And Combined Attach Reject Scenario Reasons.

Different internal or external triggers/reasons lead to 3G Attach Reject scenarios. 3G Attach Requests are rejected with network failure cause codes. New counters are added to indicate each of the different kinds of triggers. The Operator is provided the flexibility to configure the display of triggers.

Counters Track 3G Activation Failure/Reject with Cause Codes

Previous Behavior: Before this release, the existing SGSN counters did not support segregation of internal and external triggers that lead to 3G Activation Failure/Reject with cause codes. There was no break up in the SGSN code for internal and external triggers for the following cause codes that are sent out during 3G Activation Reject:

- 3G-actv-rej-network-failure
- 3G-actv-rej-svc-opt-tmp-out-of-order
- 3G-actv-rej-unspecified-error
- 3G-sec-actv-rej-unspecified-error
- 3G-actv-rej-insufficient-resources
- 3G-sec-actv-rej-insufficient-resources

New Behavior: New counters are added to indicate internal and external triggers that lead to 3G Activation Failure/Reject with cause codes. With the new counters, the operator has the flexibility to choose either internal or external triggers to compute KPIs.

custom33 Dictionary - New

A new custom33 dictionary is available. It is compliant with 3GPP TS 32.298 v.6.4.1 (custom6) with the following exceptions:

• Proprietary PLMN-ID field is present.

• It is a SEQUENCE and not a SET.

• Diagnostics and SGSN-Change fields are not supported.

• Indefinite length encoding is used.

• Booleans are encoded as 0x01(3GPP it is 0xff).

• IMEISV shall be sent if available else IMEI should be sent.

• Record Sequence Number is Mandatory.

• APN OI and NI part is length encoded.

• Cause for Record closure should be “RAT Change” instead of “intra-SGSN inter-system”.

custom33 Dictionary - IPv6 Support - Behavior Change

The SGSN now supports both IPv4 or IPv6 formats for the PDP IP address field in the S-CDR using the custom33 dictionary.

Detecting Control Plane Errors on SMC

The software has been modified to detect a catastrophic error with an internal control plane switch located on the SMC card. The system will put the failed SMC in offline state. The card with a control plane switch failure should be replaced.

The following is the log message indicating a control plane failure:

```
"The System Management Card with serial number <serial_number> in
slot <slot_number> has failed and will be reset and kept down.
(Device=SMC_GE_BCM5695, Reason=CONTROL_PLANE_MMU_FAILURE,
Status=[CPU0 MB: LINUX_RC: Done HB: xx] [CPU1 HB: xx] [CPU2]
[CPU3])".
```

Disabling ARD Checking

Checking access restriction data (ARD) in incoming insert subscriber data (ISD) messages is particularly useful in selectively restricting a subscriber in either 3G (UTRAN) or 2G (GERAN). In a previous release, the SGSN default behavior for an attach procedure was changed to check the ARD in the ISD and then accept or reject the subscriber with a configurable cause code included in the reject message.

With this release, it is now possible to disable the default behavior (ARD checking).

DLCI Utilization Counters and Statistics-

To facilitate monitoring and troubleshooting of Gb/FR E1/T1 connections, new CLI output counters have been added to measure the current and high/low watermark counters. As well, a new bulk statistics schema has been added, DLCI-Util, to monitor DLCI utilization thresholds.

DNS-SNAPTR Config CLI Moved - Behavior Change

Previous Behavior: The option to enable DNS SNAPTR for 3G subscribers with EPC subscription was under SGSN Global configuration.

New Behavior: The CLI to enable DNS SNAPTR for 3G subscribers with EPC subscription has been moved to APN Profile configuration. This will enable control of this feature per APN.

IMPORTANT

Impact on Customer: CLI configuration change required.

DSCP Marking for GTP-C Messages

The SGSN now supports diffserv code point (DSCP) marking of the GTP control plane messages on the Gn/Gp interface. This allows QoS to be set on GTP-C messages, and is useful if Gn/Gp is on a less than ideal link. DSCP marking is configurable via the CLI, with default = Best Effort Forwarding.

DSCP Template for Gb/IP

New configuration commands were added to create or remove a DSCP template which provides configuration of DSCP values for both control packets and data packets of different classes for traffic on Gb over IP.

The CLI commands which create or remove the DSCP templates are done at an SGSN-global level under the SGSN Global configuration mode; which also provides access to the new DSCP Template configuration mode.

These templates are associated with any of the configured GPRS services which allows that service to apply the configured DSCP values for all downlink packets sent out from the SGSN. If there is no profile associated with the GPRS service, the SGSN uses the default “Best Effort” DSCP values for both control and data packets.

Empty SCCP Connection Requests, Support for

The SGSN now fully supports empty SCCP Connection Requests and now adds the ability to process intra-RAU/ Detach/Service Request messages after empty CRs.

The SCCP CR messages contain the RNC’s local reference for the particular connection at the SCCP level but not any RANAP payload. Typically, the SCCP CRs will have a max payload of 130 octets with the RANAP-Initial-UE message from the RNC as the only RANAP message in the CR. The payload of the RANAP-Initial-UE can be one of the following:

- Attach with IMSI/ (P-TMSI/RAI)
- RAU with (P-TMSI/RAI)
- Service Request with P-TMSI
- Detach Request with P-TMSI

In situations where the payload exceeds 130 octets, the RNC may send an empty CR followed by the direct-transfer 1 (DT1) message with the actual payload.

Extra signalling to GGSN and MS - Behavioral Change

Previous Behavior: During a RNC initiated modification procedure if the GGSN downgrades QoS and while updating the RNC with RAB modify request if a RAB modify failure is received the GGSN and MS are not updated with the old QoS information (QoS before the GGSN downgraded the QoS).

New Behavior: During a RNC initiated modification procedure if the GGSN downgrades QoS and while updating the RNC with RAB modify request if a RAB modify failure is received the GGSN and MS are now updated with the old QoS information (QoS before the GGSN downgraded the QoS).

Full Channelization Support for NB-SS7

The grouping configuration ranges for T1 and E1 channels has been enhanced. The SGSN now supports the full 0-31 timeslots for Frame Relay (channelized) port configuration, 32 for E1 and 24 for T1.

Gb/Iu Flex Offloading Enhancements - Behavioral Change

Previously, the SGSN allowed Gb/Iu Flex subscriber offloading only as per the specification-defined NULL NRI in P-TMSI and Non-Broadcast LAC/RAC mechanism. However, not all RNCs and BSSs support NULL-NRI.

The SGSN now supports Gb/Iu Flex subscriber offloading from one SGSN to another specific SGSN in a 2G/3G pool. In addition, the operator can configure the offloading Target NRI in P-TMSI, and the quantity to off load to the Target. This can be used to provide load balancing, or to off load a single node in pool, take it out of service for whatever reason (e.g., maintenance).

GMM-SM Event Logging

To facilitate troubleshooting, the SGSN will capture procedure-level information per 2G or 3G subscriber (IMSI-based) in CSV formatted event data records (EDRs) that are stored on an external server. This feature logs the following events:

- Attaches
- Activation of PDP Context
- RAU
- ISRAU
- Deactivation of PDP Context
- Detaches
- Authentications
- PDP Modifications

The new SGSN event logging feature is enabled/disabled per service with new commands.

Gn/Gp Delay Monitoring

The SGSN can now measure the control plane packet delay for GTP-C signaling messages on the SGSN's Gn/Gp interface towards the GGSN. If the delay crosses a configurable threshold, an alarm will be generated to prompt the operator.

A delay trap is generated when the GGSN response to an ECHO message request is delayed more than a configured amount of time and for a configured number of consecutive responses. When this occurs, the GGSN will be flagged as experiencing delay.

A clear delay trap is generated when successive ECHO Response (number of successive responses to detect a delay clearance is configurable), are received from a GGSN previously flagged as experiencing delay.

This functionality can assist with network maintenance, troubleshooting, and early fault discovery.

GTP-U Echo Mechanism Enhanced - Behavior Change

Previous Behavior: If GTP-U echo was enabled, then the SGSN used GTP-U echo towards all peer GSN nodes irrespective of whether any non-DT sessions exist towards that node. In cases of GTP-U path failure, all GTP-U sessions over that path were purged.

New behavior: If GTP-U echo is enabled, the SGSN will do a GTP-U echo only when there are non- DT sessions towards a GSN/RNC. In case of GTPU path failure, only non-DT sessions are purged.

IMPORTANT

Impact on customer: If GTP-U echo is enabled, no GTP-U echo messages may be seen towards a GSN/RNC as there are no non-DT session over the path. On GTP-U path failure, DT sessions are not impacted and therefore the loss of data is less.

Handling of CAMEL Subscribers, Configurable

By default, the SGSN updates the CAMEL subscription included in the INSERT-SUBSCRIBER-DATA (ISD) messages received from the HLR. While processing the ATTACH request from the CAMEL subscriber, the SGSN checks whether it has a CAMEL service associated with the corresponding service (either GPRS service or SGN service). It drops the ATTACH request if there is no CAMEL service associated with a corresponding service.

Also by default, the SGSN does not allow establishment of a Direct Tunnel (DT) for a CAMEL subscriber. It strictly validates the subscriber against the CAMEL subscription during the Direct Tunnel setup procedure.

This enhancement makes it possible to control the behavior of the SGSN by configuring the SGSN to ignore the CAMEL subscription. This allows the SGSN to successfully complete an ATTACH procedure when there is an ATTACH Request from a CAMEL subscriber and there is no CAMEL service association in the SGSN. As well, during the Direct Tunnel establishment, validation of the CAMEL subscription is ignored to allow the DT to setup when there is no CAMEL service association in the SGSN.

Handling Multiple MS Attaches All with the Same Random TLLI

It is now possible to configure the SGSN to allow only one subscriber, at a time, to attach using a fixed random TLLI. While an Attach procedure with a fixed random TLLI is ongoing (that is, until a new P-TMSI is accepted by the MS), all other attaches sent to the SGSN with the same random TLLI, but using a different IMSI, will be dropped by the SGSN's Linkmgr.

A configurable timer has been implemented on the SGSN (invalidate old-TLLI timer) which will start upon the receipt of an Attach-Complete message with an old random TLLI. This timer will stop once an uplink packet (e.g., an Activation Request message) is received from the attached subscriber with the TLLI allocated by the SGSN. If no uplink packet is received by the subscriber with the TLLI allocated within the configured time (wait-time), the random TLLI mapping with that IMSI is freed and any other Attach Request with the

same fixed random TLLI is accepted. No further attaches from the configured fixed-random TLLI are accepted until the timer is either stopped or has expired. In addition, to limit the wait-time functionality to only the fixed random TLLI subscribers, the TLLI list can be configured to control which subscribers will be provided his functionality.

Horizontal Link Aggregation

The SGSN now supports enhanced link aggregation (LAG) within ports on different XGLCs.

LAG works by exchanging control packets (Link Aggregation Control Marker Protocol) over configured physical ports with peers to reach agreement on an aggregation of links. LAG sends and receives the control packets directly on physical ports attached to different XGLCs.

The link aggregation feature provides higher aggregated bandwidth, auto-negotiation, and recovery when a member port link goes down.

Ignoring Excess Length of Received RANAP Messages

On receiving RANAP messages from the RNC, the SGSN could experience a problem with PDP context establishment if the message is too long. Following a successful Attach, if the SGSN received a SCCP Connection Request with a GMM Service Request message from the RNC, the SGSN might respond with a SCCP Connection Refused for no clear reason. Further investigation revealed that at the RANAP layer the messages contained an Extension item, a Redirect Attempt Flag, and the SGSN reported a decode error while processing this additional octet.

Incorrect APN Handling / Default APN - Enhanced - Behavioral Change

For a PDP context request, an invalid APN occurs when none of the APNs in the HLR subscriber profile match the APN sent by the subscriber. The SGSN can now be provisioned to override an invalid APN even when a user has a wildcard APN in the HLR profile. The SGSN’s existing default APN functionality has been enhanced so that if a required subscription APN is not present in the subscriber profile, then the SGSN will now continue the activation with another configured 'dummy' APN. The call will be redirected, via the GGSN, to a Webpage informing the user of the error and prompting to subscribe for services.

Previously, if the required subscription APN was not present in subscriber profile, activation would be rejected.

Intracer invoke in 2G is disabled - Behavioral Change

Previous Behavior: Intracer is invoked for both 2G and 3G calls.

New Behavior: Intracer support is invoked only for 3G calls. Intracer support is not invoked for 2G calls and unknown subscribers (for example, unrecognized Transaction ID in case of TCAP continue message).

Lawful Intercept Buffering, Phase 2

The Lawful Intercept buffering feature has been enhanced to increase the number of call content records that can be buffered (or held in the buffer). For details, contact your local Cisco sales representative.

Local DNS --- Behavioral Change

Previously, the SGSN supported GGSN selection for an APN only through operator policy, and supported a single pool of up to 16 GGSN addresses which were selected in round robin fashion.

The SGSN now supports configuration of multiple pools of GGSNs. As part of DNS resolution, the operator can use operator policies to prioritize local GGSNs versus remote ones. This function is built upon existing load balancing algorithms in which weight and priority are configured per GGSN. With the multiple GGSN pools feature, at this time, only the weight algorithm is used for selection. So with the primary GGSN pool used first and the secondary pool used when no primary GGSNs are available.

The SGSN first selects a primary pool and then GGSNs within that primary pool; employing a round robin mechanism for selection. If none of the GGSNs in a pool are available for activation, then the SGSN proceeds with activation selecting a GGSN from a secondary pool on the basis of assigned weight. A GGSN is considered unavailable when it does not respond to GTP Requests after a configurable number of retries over a configurable time period. Path failure is detected via GTP-echo.

Local Mapping of MBR

The SGSN now provides the ability to map a maximum bit rate (MBR) value (provided by the HLR) to an HSPA MBR value. The mapped value is selected based on the matching MBR value obtained from the HLR subscription. QoS negotiation then occurs based on the converted value.

This feature is available within the operator policy framework. MBR mapping is configured via new keywords added to the qos class command in the APN Profile configuration mode. A maximum of four values can be mapped per QoS per APN.

NOTE: To enable this feature the qos prefer-as-cap, also a command in the APN Profile configuration mode, must be set to either both-hlr-and-local or to hlr subscription.

Refer to SGSN Modified Commands in the *Configuration Management* chapter of this document and to the *Cisco ASR 5000 Series Command Line Interface Reference* for details of the changes to the CLI.

Logs Enhanced To Print Additional Information

The logging level is reduced from unusual to information whenever the BSSGP layer is unable to find the GBRsap entry. Support is added to print the event, type (which prints either FR or IP), cause, nsei and nsvci information at the unusual level when the NSVC goes down at the SGSN.

Managing Path Failure Detection due to Restart Counter Change - Behavioral Change

The SGSN now provides the ability to manage GTP-C path failures detected as a result of spurious restart counter change messages received from the GGSN.

When the SGSN detects GTP-C path failure between the SGSN and the GGSN, the SGSN now assumes PDP sessions at the GGSN are lost and the SGSN deactivates those PDP sessions towards the UE with an indication that the UE should activate the PDP session again. Detection is based on receipt of restart counter change values in messages (Create PDP Context Response or Update PDP Context Response or Update PDP Context Request) which can be spurious. Potentially, this scenario can increase traffic within the operator's network.

Various enhancements have been made to manage the resulting service deactivations and activations which would cause needlessly large bursts of network traffic if the restart counter change messages from the GGSN are erroneous:

- New default behavior defined for handling GTP-C path failures detected as a result of erroneous restart counter changes received from the GGSN. See details in the Operator Notes.
- New command sets the variance allowed between values for received restart counter changes.
- New command sets the rate of PDP deactivations due to GTP-C path failures.
- New command disables the new default verification behavior.

MTP2 Parameters - Behavioral Change

Previously, the following parameters were available for configuration and for statistics display when the SS7 link was configured for low-speed:

- mtp2-eim-decrement
- mtp2-eim-increment
- mtp2-eim-threshold

Previously, the following parameters were available for configuration and for statistics display when the SS7 link was configured for high-speed:

- mtp2-aerm-emergency-threshold
- mtp2-aerm-normal-threshold
- mtp2-suerm-threshold

In accordance with specification Q.703, now EIM parameters are only available when SS7 link is configured for high-speed and AERM/SUERM parameters are only available when SS7 link is configured for low-speed.

Multiple Access 2G/3G/MME/S-GW - Limited Demo Only

The SGSN is performing trials for support of S3/S4 interfaces to enable simultaneous access between 2G and 3G networks and LTE networks with MME and S-GW.

MTP2 T2 Timer - Enhanced Range for HSL

The maximum limit for the high-speed link MTP2 T2 timer has been enhanced to 150 seconds.

Nearest GGSN Selection

Now with this feature the operator can include the RNC_ID information with the name of the APN before the query is sent to the DNS. This feature makes it possible to select a GGSN based on the RNC_ID. Name format example:

<apn_name>.<rnc_id>.<mncxxx>.<mccyyy>.gprs

With the RNC_ID inclusion enabled, the operator can also include the SCHAR (charging characteristic information) so that both the SCHAR and the RNC_ID information would be added to the name of the APN before the query is sent to the DNS. Name format example:

<apn_name>.<rnc_id>.<schar>.<mncxxx>.<mccyyy>.gprs.

Nearest GGSN Selection

It is now possible to configure the SGSN to append LAC and RAC info to an APN DNS query for GGSN selection. It is expected that the DNS will use this information to determine the GGSN to route the APN.

For example, roaming subscribers using a specific APN may want to be directed to the closest GGSN. This can be achieved by having an operator policy for roaming subscribers associated with an APN profile that includes a configuration specifying that geographical information from the LAC/RAC be appended to the APN. This is then used as the DNS query string but does not modify the APN string being sent to the GGSN.

Network Initiated PDP Context Field in S-CDR - Behavioral Change

Previous Behavior: In earlier releases, the dictionaries used by the S-CDRs included but did not implement the Network Initiated PDP Context field, hence the field was not populated.

New Behavior: Now, all the SGSN's 3GPP compliant dictionaries implement this field and the field will be populated in the following dictionaries: custom6, custom8, custom13, custom24. This field will be populated if the PDP context is activated by the network side or if the customer is enabling a RAU from LTE to 3G.

Network Overload Protection - Optimized

The SGSN's optimized network overload protection performs attach-rate throttling to avoid overloading Gr, Gn and Gf interfaces. When enabled, the IMSIMgr throttles the attach rate to a value configured with a new set of *queue-size* and *wait-time* keywords.

If the SGSN receives more than the configured number of attaches in a second, then the attaches are buffered in the pacing queue and requests are only dropped when the buffer overflows due to high incoming attach rate. Messages in the queue are processed (FIFO) until they age-out when the queued message's lifetime crosses the configured wait-time. The wait-time and the attach rate decide the optimal size of the queue.

NRI-FQDN-based DNS Resolution for non-Local RAIs

The SGSN now performs DNS query with an NRI when RAU comes from an SGSN outside the pool. The SGSN uses NRI-FQDN-based DNS resolution for the non-local RAIs for 3G subscribers in place of RAI-FQDN-based DNS resolution. This feature is enabled with a new command, refer to **`peer-nri-length`** under the *SGSN Commands - New* in the *Configuration Management* chapter.

Per RNC QoS Override - Behavior Change

Previous Behavior: Previously, there was no QoS capping for R7 RNC and capping was set at 16 mbps for all pre-R7 RNC. Bit rate override was not available.

New Behavior: Now, bit rate override is configurable per RNC. For cap rate information, refer to the **release-compliance** command information in the *Command Line Interface Reference*.

Preventing QoS Re-Negotiation Failures

Previously, when there was a change in QoS due to Inter-RAT handover from 2G to 3G OR Inter-SGSN handover with no RAB establishment, the SGSN first informs the MS of new QoS through "Modify PDP context request" and then sets up a RAB.

Now, the SGSN can initiate a RAB assignment to inform the RNC followed by UPCQ towards GGSN / Modify towards UE based on whether or not the RNC downgrades the QoS. New CLI and statistics are provided to enable this feature. By default, the SGSN informs UE before RNC.

Printing Format Changed for RAI and OLD-RAI Fields - Behavioral Change

The GMM-SM event logging feature has been enhanced so that the EDR print format is no longer fixed in length. The length is now variable. So, if the MNC has 2 digits then the RAI or OLD-RAI print format does not append a zero "0" which could cause an MNC error. During the GMM-SM event logging, the RAI and OLD-RAI fields in the EDR now have a variable length depending on the number of digits in the MNC. Based on the MNC, the

length can now be 15 (xxx-xxx-xxxx-xx) or 14 (xxx-xx-xxxx-xx) characters. For example, if MNC has 2 digits “09” then the RAI or OLD_RAI prints as - xxx-09-xxxx-xx.

PSC3 Card Qualified for SGSN

The SGSN now supports the PSC3 ***with PSC2-level capacity***. This means the PSC3 in an SGSN currently supports the same number of subscribers as the SGSN with PSC2 cards. No special configuration is required.

PSCA Supported

The SGSN now supports the PSCA. No special configuration is required.

P-TMSI Signature Reallocation - Behavioral Change

Previously, the SGSN default behavior was to allocate the P-TMSI signature.

The Cisco SGSN now supports Packet Temporary Mobile Subscriber Identity (P-TMSI) signature reallocation for all types of routing area update (RAU) events.

The P-TMSI is a temporary identity issued to a GPRS enabled mobile, unique within a given RA (routing area), and is used by the GPRS network to page the specified mobile. When enabled, the SGSN sends a P-TMSI signature to the MS in an RAU Accept message, and the MS must include the P-TMSI Signature in the next RAU request for the SGSN to compare with the original signature.

You can now configure the frequency and interval of P-TMSI signature reallocation for Periodic RAU and Normal RAU events. In this way, the SGSN can change the P-TMSI assigned to the MS as often as needed to maintain confidentiality of an MS when roaming.

P-TMSI Signature Validation Feature

When enabled, this feature allows the SGSN to send the Attach Reject for the Attach Request received with a P-TMSI signature mismatch message. This is done, primarily, to avoid the identification of incorrect mapping of P-TMSI/IMSI at the SGSN if the P-TMSI was allocated to a different MS. Enabling this feature allows the SGSN to validate the PTMSI signature present in the Attach Request against the PTMSI-SIGNATURE stored in the SGSN and then the SGSN sends the Attach Reject to the MS if the P-TMSI signature does not match.

This is applicable only for 2G attaches and this configuration forces the operator to enable P-TMSI reallocation during Attach and INTER-SGSN-RAU procedures.

qos class “all-values” - Behavioral Change

The “default” and “no” keywords in the qos class command (APN Profile configuration mode) have been replaced resulting in the following behavioral changes:

Prior to release 12, using the “default” keyword in the qos class command resulted in only a few QoS class parameters being set to predefined values and “default” was not applicable to an entire QoS class. As well, using the “no” keyword invalidated the local configuration for the entire class identified in the command.

New behavior in release 12: The new “all-values” keyword configures predefined values for all the QoS parameters within a QoS class when the keyword is invoked. Until then, there are no values configured for QoS parameters, primarily to ensure that when the QoS preference is set to “both-hlr-and-local” (since the least of the HLR and local values is considered), the SGSN does not always select the locally predefined values as they often are the lowest possible values for these parameters. This change provides a simple method to specify that all the parameters of a given QoS class, or simply to an individual, specified QoS parameter, be assigned some predefined values. The new “remove” keyword deletes the configured value(s) for an individual QoS parameter or for all parameters for a specified QoS class.

RAB Asymmetry Indicator in RAB Assignment Request

The SGSN sets the value for the RAB Asymmetry Indicator that is included in the RAB Assignment Request. The SGSN selects the value based on the symmetry of negotiated maximum bitrates as follows:

- If the uplink and downlink bitrates are equal then it is set to “Symmetric-Bidirectional”,
- If uplink bitrate is set to 0 kbps, then it is set to “Asymmetric-Unidirectional-Downlink”
- If downlink bitrate is set to 0 kbps, then it is set to “Asymmetric-Unidirectional-Uplink”
- If the uplink and downlink bitrates are non-zero and different, then it is set to “Asymmetric-Bidirectional”

A new **`rab-asymmetry-indicator`** CLI allows the SGSN to override the above functionality and set the RAB Asymmetry Indicator to “Asymmetric-Bidirectional” when uplink and downlink bitrates are equal. As a result, two sets of bitrates - one for downlink and one for uplink - will be included in the RAB Assignment Requests as mandated in 3GPP TS 25.413. For information on the new command, refer to the *Configuration Management*.

RAI IE in CPCQ/UPCQ Configurable - Behavior Change

RAI is no longer included automatically. Inclusion is operator configurable and for the following list of message types:

- 3G new SGSN RAU (change in behavior)
- 3G primary and secondary PDP activation (change in

behavior)

- 2G primary and secondary PDP activation (change in
- behavior)
- 2G new SGSN RAU
- 3G new SGSN SRNS
- 2G -> 3G HO (only if PLMN Id has changed)

- 3G -> 2G HO (only if PLMN Id has changed)
- Multiple IUPS service RAU (only if PLMN Id has
- changed)
- Multiple GPRS service RAU (only if PLMN Id has
- changed)

Reject Cause Changed from “Implicitly Detached”

Old Behavior: “Implicitly Detached” was the reject cause in the following scenario:

1. GMM cause in the reject message -- for a 3G Inter-SGSN RAU reject the cause is “Implicitly detached” when a check IMEI response timeout from the EIR occurs.
2. In the following either one of the CLI counters that gets updated in this scenario:
   - if RAU update type is PS only then Inter SGSN PS Only Routing Area Update Reject Cause counter “3G-Implicitly Detached”
   - if RAU update type is combo then Inter SGSN Comb. Routing Area Update Reject Cause counter “3G-Implicitly Detached”
3. In the following either one of the bulk statistic counters that gets updated in this scenario:
   - if RAU update type is PS only then “3G-inter-rau-rej-implicitly-detach”
   - if RAU update type is combo then “3G-comb-irau-rej-implicitly-detach”

New Behavior: The check in the code to change the GMM cause in the RAU reject message from Network failure to Implicitly detached is bypassed in the case of Inter SGSN RAU for the above said scenarios and the reject cause is changed from “Implicitly Detached” to “Network Failure”:

1. GMM cause in the reject message -- for a 3G Inter-SGSN RAU reject the cause is “Network Failure” when a check IMEI response timeout from the EIR occurs.
2. In the following either one of the CLI counters that gets updated in this scenario:
   - if RAU update type is PS only then Inter SGSN PS Only Routing Area Update Reject Cause counter “3G- Network Failure”
   - if RAU update type is combo then Inter SGSN Comb. Routing Area Update Reject Cause counter “3G- Network Failure”
3. In the following either one of the bulk statistic counters that gets updated in this scenario:
   - if RAU update type is PS only then “3G-inter-rau-rej-network-failure”
   - if RAU update type is combo then “3G-comb-irau-rej-network-failure”

Impact on Customer: The customer might see an increase in the network failure counter rather than in the implicitly detached counter for such above said scenarios.

Reordering of SNDCP N-PDU Segments - Behavior Change

In previous releases, the SGSN partially supported reordering out-of-order segments coming from the same SNDCP N-PDU. If the first N-PDU segment came after subsequent segments, then the entire N-PDU was dropped.

Now, the SGSN fully supports reordering out-of-order segments coming from the same SNDCP N-PDU. The SGSN waits the configured amount of time for all segments of the N-PDU to arrive. If all the segments are not received before the timer expiries, then all queued segments are dropped.

Replacement of “IMEI Black Listed” Counter

Previous Behavior: “IMEI Black Listed” counter pegged the IMEI being black listed at the EIR and also network/response timeout failures.

New Behavior: A new counter, “Check IMEI Failure” counter pegs for IMEI being black listed at the EIR and for all types of failures at the EIR such as response timeout/network failure.

Re-Transmitted Secondary PDP CR Messages

Previous Behavior: In 2G scenarios, the SGSN clears the original call to receive re-transmitted Activate PDP context request message. The SGSN incorrectly treats the re-transmitted request as a new activate request with some parameters same as the original activation request.

New Behavior: If the new activate PDP request is same as the on-going activation request it indicates that the new request is a re-transmitted request, the SGSN drops such re-transmitted activation requests and continues with the on-going activation request.

‘Roaming Not Allowed’ Configurable Cause for GMM-Rejects

It is now possible for the operator to configure the desired reject cause code for ‘roaming-not-allowed’ when sending GMM-Reject to the UE. Cause options include:

- gprs-serv-and-non-gprs-serv-not-allowed
- gprs-serv-not-allowed
- gprs-serv-not-in-this-plmn
- location-area-not-allowed
- network-failure
- no-suitable-cell-in-this-la
- plmn-not-allowed
- roaming-not-allowed-in-this-la

For the new command to configure, see the new **`local-cause-code-mapping`** command in the *Configuration Management* chapter.

S6d DIAMETER Interface Support - Limited Demo Only

The SGSN is trailing support for the S6d interface between the SGSN and the HSS. This will enable the SGSN to get subscription details of a 4G user from the HSS when user tries

to register with the SGSN, either as part of an Inter-RAT handoff from 4G, or while attaching into 3G or 2G access.

SCTP Configuration Applied for Cross Path Connections

Previous Behavior: SCTP configurations were not applied for cross path connections.

New Behavior: New default behavior is for SCTP configurations to be applied for cross path connections.

SCTP Timing Granularity Enhanced

The SGSN now allows settings to be configured with finer granularity for several of the SCTP timers:

- Minimum SCTP Retransmission Timeout (sctp-rto-min)
- Selective ACK Period (sctp-sack-period)

This can improve interoperability with certain RAN equipment.

SMS Authentication Repetition Rate - Behavioral Change

Previously, the SGSN provides an authentication procedures for standard GMM events like Attach, Detach, RAU, and Service-Request, and SMS events such as Activate, all with support for 1-in-N Authenticate functionality. The SGSN did not provide the capability to authenticate MO/MT SMS events.

Now, the authentication functionality has been expanded to the Gs interface where the SGSN now supports configuration of the authentication repetition rate for SMS-MO and SMS-MT, for every nth event. This functionality is built on existing SMS CLI, with configurable MO and/or MT. The default is not to authenticate.

SMSC Address Denial - Behavioral Change

Previously, the SGSN supported restricting MO-SMS and MT-SMS only through SGSN operator policy configuration.

Now, the SGSN can restrict forwarding of SMS messages to specific SMSC addresses, in order to allow operators to block SMS traffic that cannot be charged for. This functionality supports multiple SMSCs and is configurable per SMSC address with a maximum of 10 addresses. It is also configurable for MO-SMS and/or MT-SMS messages.

SONET APS and SDH MSP (1+1) Inter-Card Support on OLC2

Automatic Protection Switching (APS) is the ability of the system to detect failures on a working facility and switch to a designated backup facility. The failures are detected in the Multiplex Section of the SDH Overhead (MSOH) or Section Overhead (SOH) of SONET.

The SGSN now provides inter-card support of SONET APS and MSP (Multiplexed Switching Protection) functionality on the Optical Line Card 2 (OLC2) as specified in G.783 Annex A.

Supporting/non-Supporting UE for Attach and RAU - Behavior Change

Previous Behavior: The SGSN believed the UE could be classified as supporting or non-supporting only during Attach.

New Behavior: Now, the SGSN classifies the UE as supporting or non-supporting UE for either Attach or RAU.

Threshold for Additional Authentication Vectors

The software has been enhanced to allow the operator to configure a threshold indicating the minimum number of unused vectors that should be maintained by the SGSN before it initiates a SAI to refill the buffer. With this feature enabled, the SGSN will maintain a specific number of unused vectors at all times. The SAI is initiated when a vector is used up by the SGSN for authentication and the configuration threshold is hit. The SAI initiated, due to this configuration, will be ongoing in parallel to the procedures. This feature changes how many vectors are retrieved from the HLR each time and stored on the SGSN so it should increase performance by decreasing the amount of interaction with the HLR during procedures.

Trap for non-Receipt of Reset-ACK - Behavior Change

Previous Behavior: The SGSN was not generating traps if Reset-ACK was not received from the RNC. The SGSN was logging not having received a Reset-ACK.

New Behavior: Now, upon expiry of all retransmission timers for reset from the SGSN, the SGSN will generate a visible trap and make a log entry when Reset-ACK is not received. The new trap is of type Notification, so there is no clear trap operation required.

ULI IE in GTP Messages

Previous Behavior: For a 3G session, a ULI IE was always included in Create/Update PDP Context Request messages if the “gtp send uli” option was enabled in the call control profile.

New Behavior: Including of ULI IE in GTP messages is now conditional and depends on whether the correct SAI is available. For a 3G session, if the “gtp send uli” option is enabled in a call control profile, then:

• “ULI IE is always included in a Create PDP Context Request, but ('but' may not be needed, you take a call)

• “ULI IE is included in the Update PDP Context Request except during Inter SGSN / Intra SGSN SRNS and PDP Context Preservation procedures.

• “Also, additional Update PDP Context Request may be sent with ULI IE, whenever an Inter / Intra SGSN SRNS is followed by a RAU.

• “In general, ULI IE is included in Update PDP Context Request only if the correct SAI information is available at the SGSN.

Impact on Customer: The customer may experience an increase in Update PDP Context Request & Response messages. SAI within ULI IE will always be valid and will reflect the current location of the MS.

Verification of EDR GMM-SM Event Logs

New counters have been added for 2G Modify PDP Abort and for 3G Modify Abort. The new counters facilitate verification of the EDR GMM-SM event logs.

SGSN Features in Release 12.1

This section provides information on new Serving GPRS Support Node (SGSN) features in Release 12.1. Additional information on these features can be found in the *SGSN Administration Guide*, and in the *Command Line Interface Reference*.

Max Number of LACs Configurable for Gs Service Increased

The configuration limits have increased from 32 to 128 for the maximum number of LACs, as a combined total for LACs configured, for pool-areas and non-pool-areas for a Gs Service.

Max Number of LACs / Zone Code List - Behavioral Change

Maximum number of LACs per allowed zone code list has increased from 10 to 100.

3GPP 23.008 Regional Subscription Information (RSZI)

The SGSN now fully supports regional subscription zone identities (RSZIs) in accordance with TS 23.008. The HLR stores a list of RSZIs; 10 per network destination code (NDC). The RSZI are comprised of the PLMN id and the zone code lists. The SGSN now enables the operator to define the zone code lists, to enable zone code checking, and to define the cause code for subscription rejection when it is due to regional subscription information failure.

3G NRPCA

The SGSN now supports the Network Requested PDP Context Activation (NRPCA) procedure for 3G attachments. Whenever there is downlink data at the GGSN for a subscriber, but there is no valid context for the already-established PDP address, the GGSN initiates an NRPCA procedure towards the SGSN. Prior to starting the NRPCA procedure, the GGSN either obtains the SGSN address from the HLR or uses the last SGSN address of

the subscriber available at the GGSN. There are no interface changes to support this feature. Support is configured with existing CLI commands (network-initiated-pdp-activation, location-area-list) in the call-control-profile configuration mode and timers (T3385-timeout and max-actv-retransmission) are set in the SGSN service configuration mode.

APN Handling / Default APN - Enhanced

For a PDP context request, an invalid APN occurs when none of the APNs in the HLR subscriber profile match the APN sent by the subscriber. The SGSN can now be provisioned to override an invalid APN even when a user has a wildcard APN in the HLR profile. The SGSN's existing default APN functionality has been enhanced so that if a required subscription APN is not present in the subscriber profile, then the SGSN will now continue the activation with another configured 'dummy' APN. The call will be redirected, via the GGSN, to a Webpage informing the user of the error and prompting to subscribe for services.

Previously, if the required subscription APN was not present in subscriber profile, activation would be rejected.

APN Override Enhancements

The SGSN now provides the ability to configure default APN to be used in several different scenarios:

• Use the APN in the first subscription record as a default APN. With this option the first subscription record with matching PDP type and PDP address will be used as the default APN. Here, first record means the first among the records received from HLR in that order. The default APN will be used if normal APN selection fails. This function is enabled via the new key-word '**`first-in-subscription`**'.

• Fallback to the APN in the first subscription record when configured default APN is not available. It is possible to configure a default APN to be used. However, if the configured default APN is not present in subscription then the SGSN will use the APN in the first subscription record with matching PDP type and PDP address. This function is enabled via the new keyword '**`fallback-to-first-in-subscription`**'.

• Prefer to use a single subscription record option, which specifies that if normal APN selection fails and if there is only one subscription record, then use the APN in that subscription record as the default APN. This is an optional configuration and is specified along with a default APN to be used. The configured default APN will be used when there are more than one subscription records. This feature is enabled via the new keyword '**`prefer-single-subscription`**'.

Controlling THP and ARP via Operator Policy

The SGSN's local QoS THP and ARP configurations can now override the QoS traffic handling priority (THP) value and allocation/retention priority (ARP) from an HLR subscription. This QoS capping can be done on a per-APN basis and is configurable in the APN profile for use through the operator policy function.

This functionality can differentiate home vs. roaming subscribers, and prevent visiting subscribers from receiving a high-tiered service. For example, a service provider could offer service differentiation using Ultra/Super/Standard service levels based upon QoS; this could justify charging a corporate customer more to use the Internet APN than would be charged to a consumer. This could be accomplished by controlling the traffic handling priority (THP) over the air interface, i.e. THP 1 = Ultra, THP 2 = Super and THP 3 = Standard. But this must be configured at the operator policy level to prevent a “roamed-in” customer from getting Ultra service if the foreign subscriber’s network provisions all of their customers with THP 1 on their HLRs.

custom33 Dictionary - New

A new custom33 dictionary is available. It is compliant with 3GPP TS 32.298 v.6.4.1 (custom6) with the following exceptions:

- Proprietary PLMN-ID field is present.
- It is a SEQUENCE and not a SET.
- Diagnostics and SGSN-Change fields are not supported.
- Indefinite length encoding is used.
- Booleans are encoded as 0x01(3GPP it is 0xff).
- IMEISV shall be sent if available else IMEI should be sent.
- Record Sequence Number is Mandatory.
- APN OI and NI part is length encoded.
- Cause for Record closure should be “RAT Change” instead of “intra-SGSN inter-system”.

Disabling ARD Checking

Checking access restriction data (ARD) in incoming insert subscriber data (ISD) messages is particularly useful in selectively restricting a subscriber in either 3G (UTRAN) or 2G (GERAN). In a previous release, the SGSN default behavior for an attach procedure was changed to check the ARD in the ISD and then accept or reject the subscriber with a configurable cause code included in the reject message.

With this release, it is now possible to disable the default behavior (ARD checking).

DSCP Marking for GTP-C Messages

The SGSN now supports diffserv code point (DSCP) marking of the GTP control plane messages on the Gn/Gp interface. This allows QoS to be set on GTP-C messages, and is useful if Gn/Gp is on a less than ideal link. DSCP marking is configurable via the CLI, with default = Best Effort Forwarding.

Full Channelization Support for NB-SS7

The grouping configuration ranges for T1 and E1 channels has been enhanced. The SGSN now supports the full 0-31 timeslots for Frame Relay (channelized) port configuration, 32 for E1 and 24 for T1.

Gb/Iu Flex Offloading Enhancements - Behavioral Change

Previously, the SGSN allowed Gb/Iu Flex subscriber offloading only as per the specification-defined NULL NRI in P-TMSI and Non-Broadcast LAC/RAC mechanism. However, not all RNCs and BSSs support NULL-NRI.

The SGSN now supports Gb/Iu Flex subscriber offloading from one SGSN to another specific SGSN in a 2G/3G pool. In addition, the operator can configure the offloading Target NRI in P-TMSI, and the quantity to off load to the Target. This can be used to provide load balancing, or to off load a single node in pool, take it out of service for whatever reason (e.g., maintenance).

Gn/Gp Delay Monitoring

The SGSN can now measure the control plane packet delay for GTP-C signaling messages on the SGSN's Gn/Gp interface towards the GGSN. If the delay crosses a configurable threshold, an alarm will be generated to prompt the operator.

A delay trap is generated when the GGSN response to an ECHO message request is delayed more than a configured amount of time and for a configured number of consecutive responses. When this occurs, the GGSN will be flagged as experiencing delay.

A clear delay trap is generated when successive ECHO Response (number of successive responses to detect a delay clearance is configurable), are received from a GGSN previously flagged as experiencing delay.

This functionality can assist with network maintenance, troubleshooting, and early fault discovery.

Horizontal Link Aggregation

The SGSN now supports enhanced link aggregation (LAG) within ports on different side-by-side XGLCs. Ports can be from multiple XGLCs with some cards in L2 (side-by-side) redundancy.

LAG works by exchanging control packets (Link Aggregation Control Marker Protocol) over configured physical ports with peers to reach agreement on an aggregation of links. LAG sends and receives the control packets directly on physical ports attached to different XGLCs.

The link aggregation feature provides higher aggregated bandwidth, auto-negotiation, and recovery when a member port link goes down. With side-by-side redundancy on the XGLC, link aggregation supports horizontal ports from both XGLC cards.

Incorrect APN Handling / Default APN - Enhanced - Behavioral Change

For a PDP context request, an invalid APN occurs when none of the APNs in the HLR subscriber profile match the APN sent by the subscriber. The SGSN can now be provisioned to override an invalid APN even when a user has a wildcard APN in the HLR profile. The SGSN's existing default APN functionality has been enhanced so that if a required subscription APN is not present in the subscriber profile, then the SGSN will now continue the activation with another configured 'dummy' APN. The call will be redirected, via the

GGSN, to a Webpage informing the user of the error and prompting to subscribe for services.

Previously, if the required subscription APN was not present in subscriber profile, activation would be rejected.

Lawful Intercept Buffering, Phase 2

The Lawful Intercept buffering feature has been enhanced to increase the number of call content records that can be buffered (or held in the buffer). For details, refer to the ASR 5000 Series Lawful Intercept Configuration Guide.

Local DNS --- Behavioral Change

Previously, the SGSN supported GGSN selection for an APN only through operator policy, and supported a single pool of up to 16 GGSN addresses which were selected in round robin fashion.

The SGSN now supports configuration of multiple pools of GGSNs. As part of DNS resolution, the operator can use operator policies to prioritize local GGSNs versus remote ones. This function is built upon existing load balancing algorithms in which weight and priority are configured per GGSN. With the multiple GGSN pools feature, at this time, only the weight algorithm is used for selection. So with the primary GGSN pool used first and the secondary pool used when no primary GGSNs are available.

The SGSN first selects a primary pool and then GGSNs within that primary pool; employing a round robin mechanism for selection. If none of the GGSNs in a pool are available for activation, then the SGSN proceeds with activation selecting a GGSN from a secondary pool on the basis of assigned weight. A GGSN is considered unavailable when it does not respond to GTP Requests after a configurable number of retries over a configurable time period. Path failure is detected via GTP-echo.

Local Mapping of MBR

The SGSN now provides the ability to map a maximum bit rate (MBR) value (provided by the HLR) to an HSPA MBR value. The mapped value is selected based on the matching MBR value obtained from the HLR subscription. QoS negotiation then occurs based on the converted value.

This feature is available within the operator policy framework. MBR mapping is configured via new keywords added to the qos class command in the APN Profile configuration mode. A maximum of four values can be mapped per QoS per APN.

NOTE: To enable this feature the qos prefer-as-cap, also a command in the APN Profile configuration mode, must be set to either both-hlr-and-local or to hlr subscription.

Refer to SGSN Modified Commands in the *Configuration Management* chapter of this document and to the *Cisco ASR 5000 Series Command Line Interface Reference* for details of the changes to the CLI.

MTP2 Parameters - Behavioral Change

Previously, the following parameters were available for configuration and for statistics display when the SS7 link was configured for low-speed:

- mtp2-eim-decrement
- mtp2-eim-increment
- mtp2-eim-threshold

Previously, the following parameters were available for configuration and for statistics display when the SS7 link was configured for high-speed:

- mtp2-aerm-emergency-threshold
- mtp2-aerm-normal-threshold
- mtp2-suerm-threshold

In accordance with specification Q.703, now EIM parameters are only available when SS7 link is configured for high-speed and AERM/SUERM parameters are only available when SS7 link is configured for low-speed.

Multiple Access 2G/3G/MME/S-GW - Limited Demo Only

The SGSN is performing trials for support of S3/S4 interfaces to enable simultaneous access between 2G and 3G networks and LTE networks with MME and S-GW.

MTP2 T2 Timer - Enhanced Range for HSL

The maximum limit for the high-speed link MTP2 T2 timer has been enhanced to 150 seconds.

PSC3 Card Qualified for SGSN

The SGSN now supports the PSC3 ***with PSC2-level capacity***. This means the PSC3 in an SGSN currently supports the same number of subscribers as the SGSN with PSC2 cards. No special configuration is required.

PSCA Supported

The SGSN now supports the PSCA. No special configuration is required.

P-TMSI Signature Reallocation - Behavioral Change

Previously, the SGSN default behavior was to allocate the P-TMSI signature.

The Cisco SGSN now supports Packet Temporary Mobile Subscriber Identity (P-TMSI) signature reallocation for all types of routing area update (RAU) events.

The P-TMSI is a temporary identity issued to a GPRS enabled mobile, unique within a given RA (routing area), and is used by the GPRS network to page the specified mobile. When enabled, the SGSN sends a P-TMSI signature to the MS in an RAU Accept message, and the MS must include the P-TMSI Signature in the next RAU request for the SGSN to compare with the original signature.

You can now configure the frequency and interval of P-TMSI signature reallocation for Periodic RAU and Normal RAU events. In this way, the SGSN can change the P-TMSI assigned to the MS as often as needed to maintain confidentiality of an MS when roaming.

qos class “all-values” - Behavioral Change

The “default” and “no” keywords in the qos class command (APN Profile configuration mode) have been replaced resulting in the following behavioral changes:

Prior to release 12, using the “default” keyword in the qos class command resulted in only a few QoS class parameters being set to predefined values and “default” was not applicable to an entire QoS class. As well, using the “no” keyword invalidated the local configuration for the entire class identified in the command.

New behavior in release 12: The new “all-values” keyword configures predefined values for all the QoS parameters within a QoS class when the keyword is invoked. Until then, there are no values configured for QoS parameters, primarily to ensure that when the QoS preference is set to “both-hlr-and-local” (since the least of the HLR and local values is considered), the SGSN does not always select the locally predefined values as they often are the lowest possible values for these parameters. This change provides a simple method to specify that all the parameters of a given QoS class, or simply to an individual, specified QoS parameter, be assigned some predefined values. The new “remove” keyword deletes the configured value(s) for an individual QoS parameter or for all parameters for a specified QoS class.

RAI IE in CPCQ/UPCQ Configurable - Behavior Change

RAI is no longer included automatically. Inclusion is operator configurable and for the following list of message types:

- 3G new SGSN RAU (change in behavior)
- 3G primary and secondary PDP activation (change in behavior)
- 2G primary and secondary PDP activation (change in behavior)
- 2G new SGSN RAU
- 3G new SGSN SRNS
- 2G -> 3G HO (only if PLMN Id has changed)
- 3G -> 2G HO (only if PLMN Id has changed)
- Multiple IUPS service RAU (only if PLMN Id has changed)
- Multiple GPRS service RAU (only if PLMN Id has changed)

Reordering of SNDCP N-PDU Segments - Behavioral Change

In previous releases, the SGSN partially supported reordering out-of-order segments coming from the same SNDCP N-PDU. If the first N-PDU segment came after subsequent segments, then the entire N-PDU was dropped.

Now, the SGSN fully supports reordering out-of-order segments coming from the same SNDCP N-PDU. The SGSN waits the configured amount of time for all segments of the N-PDU to arrive. If all the segments are not received before the timer expiries, then all queued segments are dropped.

S6d DIAMETER Interface Support - Limited Demo Only

The SGSN is trailing support for the S6d interface between the SGSN and the HSS. This will enable the SGSN to get subscription details of a 4G user from the HSS when user tries to register with the SGSN, either as part of an Inter-RAT handoff from 4G, or while attaching into 3G or 2G access.

SCTP Timing Granularity Enhanced

The SGSN now allows settings to be configured with finer granularity for several of the SCTP timers:

- Minimum SCTP Retransmission Timeout (sctp-rto-min)
- Selective ACK Period (sctp-sack-period)

This can improve interoperability with certain RAN equipment.

SMS Authentication Repetition Rate - Behavioral Change

Previously, the SGSN provides an authentication procedures for standard GMM events like Attach, Detach, RAU, and Service-Request, and SMS events such as Activate, all with support for 1-in-N Authenticate functionality. The SGSN did not provide the capability to authenticate MO/MT SMS events.

Now, the authentication functionality has been expanded to the Gs interface where the SGSN now supports configuration of the authentication repetition rate for SMS-MO and SMS-MT, for every nth event. This functionality is built on existing SMS CLI, with configurable MO and/or MT. The default is not to authenticate.

SMSC Address Denial - Behavioral Change

Previously, the SGSN supported restricting MO-SMS and MT-SMS only through SGSN operator policy configuration.

Now, the SGSN can restrict forwarding of SMS messages to specific SMSC addresses, in order to allow operators to block SMS traffic that cannot be charged for. This functionality supports multiple SMSCs and is configurable per SMSC address with a maximum of 10 addresses. It is also configurable for MO-SMS and/or MT-SMS messages.

SONET APS and SDH MSP (1+1) Inter-Card Support on OLC2

Automatic Protection Switching (APS) is the ability of the system to detect failures on a working facility and switch to a designated backup facility. The failures are detected in the Multiplex Section of the SDH Overhead (MSOH) or Section Overhead (SOH) of SONET.

The SGSN now provides inter-card support of SONET APS and MSP (Multiplexed Switching Protection) functionality on the Optical Line Card 2 (OLC2) as specified in G.783 Annex A.

SGSN Features in Release 12.2

This section provides information on new Serving GPRS Support Node (SGSN) features in Release 12.2. Additional information on these features can be found in the *SGSN Administration Guide*, and in the *Command Line Interface Reference*.

Actions per GTT Association

The maximum number of actions per GTT association has been increased from 8 to 15.

APN Remapping Based on Charging Characteristics - Behavioral Change

Previous Behavior: The original APN remapping behavior was such that if any of the subscription record had matching charging characteristics then the requested APN would be remapped to the configured APN <*apn_net_id*>.

New Behavior: APN remapping behavior has been modified so that remapping occurs only when the charging characteristics value in the subscription record associated with the requested APN matches the configured value. This will avoid remapping of all APNs that the subscriber requests. This change is implemented with the new **new-ni** keyword of the **cc** command in the APN Remap Table configuration mode - explained in “Modified Commands” section of the *Configuration Management* chapter.

BVC Reset Handling - Behavioral Change

Previous Behavior: When a BVC was mapped to a specific cell-ID and the SGSN received a BVC Reset with a different cell-ID, then a new entry was added in the mapping for the new BVCI but the old mapping entry was not deleted. The BVCI of the subscriber was not updated until the SGSN received the next uplink packet from the MS.

New Behavior: The SGSN maintains BVC to cell-ID mapping. When a BVC is mapped to a specific cell-ID and the SGSN receives a BVC Reset with a different cell-ID, then a new entry is added in the mapping for the new BVCI. The BVCI of the subscriber is updated and the old mapping entry is deleted.

APN Selection of GGSN/PGW based on Network Capability - Behavioral Change

Previous Behavior: The SGSN could only select a GGSN (perform only DNS “A” queries).

New Behavior: The SGSN can also perform a DNS “SNAPTR” type (Straightforward Name Authority Pointer) query to select a PGW if the mobile UE is Release 9 compliant.

The Gn/Gp SGSN can now be configured to select a combined PGW/GGSN node to anchor a PDP context. During PDP context activation, after the APN is selected, normally a Gn/Gp SGSN does a DNS A/AAA query to resolve the APN into a GGSN IP address. Now, if the MS and the network are both EPC-capable, then the Gn/Gp SGSN should select a combined PGW/GGSN node to anchor the PDP context. This will enable the subscriber to roam into an EPC network without losing the PDP context.

In order to support PGW selection for an MS that is EPC capable, an SGSN shall do a DNS SNAPTR query for APN resolution.

If this feature is not enabled on the SGSN, the SGSN proceeds with the selection of a GGSN as usual, despite the UE ‘s network capability. Without this feature, whenever a release 9 compliant UE moves from a 2G/3G network to a 4G network, the PDP context has to be deactivated from the GGSN and a new activation towards a PGW is needed.

With this feature enabled, the signaling load on the network side is reduced because the deactivation and activation procedure is avoided when the SGSN selects a PGW during 2G/3G activation.

Configurable SCTP Receiver Window Size - Behavior Change

It is now possible for the operator to configure a reduced priority for Link Manager Control messages, thereby giving timer messages the highest priority. The timer messages are retained at the highest priority and data messages are kept at a lower priority. As a part of this enhancement, a new parameter, **`sctp-init-rwnd`**, will enable the SCTP association to maintain a configurable window at the receiving end.

Configurable Start for MS Authentication on First Vector

To avoid high traffic levels during PDP establishment, the SGSN has been modified to reduce the attach time, as much as possible, so that the devices can attach and discontinue sending requests. This change is intended to reduce the time needed to retrieve vectors over the Gr interface by allowing the operator to configure the SGSN to start authentication towards the MS as soon as it receives the first vector from the AuC/HLR. With the change to the configuration, the SGSN begins the MS authentication process immediately after receiving the first vector from the HLR, while the SAI continues in parallel.

Continue with Attach when EIR is Unreachable

The attach process may continue in the case of an IMEI check timeout, based on the SGSN service and/or the GPRS service configuration. But the attach only proceeds if the route towards the EIR is up and the IMEI request timer expires.

The software has been enhanced to configure the SGSN to allow the attach process to continue if the route towards the EIR is down, e.g., the DPC / SSN is out of service. This new CLI control command has been added to SGSN service and GPRS service configuration modes.

Continuous File Sequence Numbers for S-CDR

A file sequence number is a unique number assigned to an individual CDR file. This file sequence number is stored in the aaaproxy and if the aaaproxy restarts or the chassis restarts then the sequence number used to reset. This feature prevents the file sequence number from resetting to zero and recovers the file sequence number so that the number continues to be incremented.

The file sequence number is stored in RAM and whenever a file is transferred from RAM to the hard disk drive (HDD on the SMC), the file containing the latest sequence number is also sent to the HDD.

custom29 Dictionary - New

The custom29 dictionary has been implemented in compliance with 3GPP 32.215 v4.5.0 to provide standard Release 4 format for S-CDRs with all IP addresses in binary format. This implementation follows standards with the following exceptions:

• The MSISDN field does not include the Nature of Address and Numbering Plan indicators.

• The QoS length should be restricted to 12 bytes.

custom33 Dictionary - IPv6 Support - Behavior Change

The SGSN now supports both IPv4 or IPv6 formats for the PDP IP address field in the S-CDR using the custom33 dictionary.

DLCI Utilization Counters and Statistics

To facilitate monitoring and troubleshooting of Gb/FR E1/T1 connections, new CLI output counters have been added to measure the current and high/low watermark counters. As well, a new bulk statistics schema has been added, DLCI-Util, to monitor DLCI utilization thresholds.

Dual PDP Address (IPv4v6) Support for Gn/Gp

In accordance with 3GPP TS24.008, TS23.060, and TS29.060 Release 9.0 specifications, the SGSN now honors MS/UE requests for dual PDP type addressing (IPv4v6) for PDP context association with one IPv4 address and one IPv6 address/prefix.

It is now possible, to configure SGSN support for MS/UE requested dual PDP type addressing (IPv4v6) for PDP context association with one IPv4 address and one IPv6 address/prefix. Once support is configured for the entire SGSN, the operator has multiple configurable options to refine the level of support for dual PDP type addressing:

- Disable SGSN support for dual PDP type addressing.
- Disable support at the RNC-level for a specific RNC that either does or does not support this type of addressing.
- Configure the SGSN to override the MS/UE requested IPv4v6 PDP type, if SGSN does not support IPv4v6, on the basis of APN selection.
- Configure a default APN with a wildcard subscription with PDP type IPv4v6.

Empty SCCP Connection Requests, Support for

The SGSN now fully supports empty SCCP Connection Requests and now adds the ability to process intra-RAU/ Detach/Service Request messages after empty CRs.

The SCCP CR messages contain the RNC's local reference for the particular connection at the SCCP level but not any RANAP payload. Typically, the SCCP CRs will have a max payload of 130 octets with the RANAP-Initial-UE message from the RNC as the only RANAP message in the CR. The payload of the RANAP-Initial-UE can be one of the following:

- Attach with IMSI/ (P-TMSI/RAI)
- RAU with (P-TMSI/RAI)
- Service Request with P-TMSI
- Detach Request with P-TMSI

In situations where the payload exceeds 130 octets, the RNC may send an empty CR followed by the direct-transfer 1 (DT1) message with the actual payload.

GMM-SM Event Logging

To facilitate troubleshooting, the SGSN will capture procedure-level information per 2G or 3G subscriber (IMSI-based) in CSV formatted event data records (EDRs) that are stored on an external server. This feature logs the following events:

- Attaches
- Activation of PDP Context
- RAU
- ISRAU
- Deactivation of PDP Context
- Detaches
- Authentications
- PDP Modifications

The new SGSN event logging feature is enabled/disabled per service with new commands.

GTPU Filter for IuPS and SGTP Service Information - Behavioral Change

Previous Behavior: The SGSN performed GTP protocol user plane (GTPU) path management per remote node. Paths (connection between two endpoints identified by IP addresses) were not monitored individually. In case of GTPU path failure, all PDPs associated with the remote node were deleted.

New Behavior: By default, GTPU path management is now done per path. The SGSN tracks the PDPs towards the GGSN and the RABs towards the RNC on a per path basis. This makes it possible to list all paths towards a remote node and perform path analysis. As well, in case of path failure, only the PDP contexts and RABs associated with the failed path are affected.

Handling of CAMEL Subscribers, Configurable

By default, the SGSN updates the CAMEL subscription included in the INSERT-SUBSCRIBER-DATA (ISD) messages received from the HLR. While processing the ATTACH request from the CAMEL subscriber, the SGSN checks whether it has a CAMEL service associated with the corresponding service (either GPRS service or SGN service). It drops the ATTACH request if there is no CAMEL service associated with a corresponding service.

Also by default, the SGSN does not allow establishment of a Direct Tunnel (DT) for a CAMEL subscriber. It strictly validates the subscriber against the CAMEL subscription during the Direct Tunnel setup procedure.

This enhancement makes it possible to control the behavior of the SGSN by configuring the SGSN to ignore the CAMEL subscription. This allows the SGSN to successfully complete an ATTACH procedure when there is an ATTACH Request from a CAMEL subscriber and there is no CAMEL service association in the SGSN. As well, during the Direct Tunnel establishment, validation of the CAMEL subscription is ignored to allow the DT to setup when there is no CAMEL service association in the SGSN.

Handling inter-SGSN/inter-system Suspend (2G) - Behavioral Change

Previous Behavior: The SGSN only handled Suspend messages received for a known MS with a RA configured in the SGSN's GPRS service configuration. However, the response to Suspend messages received with a 3G RA or unknown RA was to send Suspend-NAK.

New Behavior: Upon reception of Suspend, the old SGSN suspends data transmission towards the UE and typically starts buffering of packets to ensure these packets are not sent towards the RAN node where they might be lost because the subscriber has moved to the coverage of a different SGSN. The SGSN does not initiate Paging for a suspended MS and waits for the MS to send RAU Request/Resume to resume GPRS service.

In accordance with 3GPP TS 23.060 16.2.1.1.1, the SGSN responds to received Suspend messages in the following manner:

- **Inter-SGSN-Suspend:** the SGSN forwards inter-SGSN Suspend Request to the old SGSN (derived using the RA in the Suspend Request), and then sends Suspend-Ack upon receiving Suspend-Ack from the old SGSN.
- **Intra-SGSN-Inter-RAT-Suspend:** the SGSN sends SRNS-Ctxt-Request to the RNC upon receiving inter-system Suspend Request, and then sends Suspend-Ack upon receiving SRNS-Ctxt-Response from the RNC.

Handling Multiple MS Attaches All with the Same Random TLLI

It is now possible to configure the SGSN to allow only one subscriber, at a time, to attach using a fixed random TLLI. While an Attach procedure with a fixed random TLLI is ongoing (that is, until a new P-TMSI is accepted by the MS), all other attaches sent to the SGSN with the same random TLLI, but using a different IMSI, will be dropped by the SGSN's Linkmgr.

A configurable timer has been implemented on the SGSN (invalidate old-TLLI timer) which will start upon the receipt of an Attach-Complete message with an old random TLLI. This timer will stop once an uplink packet (e.g., an Activation Request message) is received from the attached subscriber with the TLLI allocated by the SGSN. If no uplink packet is received by the subscriber with the TLLI allocated within the configured time (wait-time), the random TLLI mapping with that IMSI is freed and any other Attach Request with the same fixed random TLLI is accepted. No further attaches from the configured fixed-random TLLI are accepted until the timer is either stopped or has expired. In addition, to limit the wait-time functionality to only the fixed random TLLI subscribers, the TLLI list can be configured to control which subscribers will be provided his functionality.

Ignoring Excess Length of Received RANAP Messages

On receiving RANAP messages from the RNC, the SGSN could experience a problem with PDP context establishment if the message is too long. Following a successful Attach, if the SGSN received a SCCP Connection Request with a GMM Service Request message from the RNC, the SGSN might respond with a SCCP Connection Refused for no clear reason. Further investigation revealed that at the RANAP layer the messages contained an Extension item, a Redirect Attempt Flag, and the SGSN reported a decode error while processing this additional octet.

Managing Path Failure Detection due to Restart Counter Change - Behavioral Change

The SGSN now provides the ability to manage GTP-C path failures detected as a result of spurious restart counter change messages received from the GGSN.

When the SGSN detects GTP-C path failure between the SGSN and the GGSN, the SGSN now assumes PDP sessions at the GGSN are lost and the SGSN deactivates those PDP sessions towards the UE with an indication that the UE should activate the PDP session again. Detection is based on receipt of restart counter change values in messages (Create PDP Context Response or Update PDP Context Response or Update PDP Context Request) which can be spurious. Potentially, this scenario can increase traffic within the operator's network.

Various enhancements have been made to manage the resulting service deactivations and activations which would cause needlessly large bursts of network traffic if the restart counter change messages from the GGSN are erroneous:

- New default behavior defined for handling GTP-C path failures detected as a result of erroneous restart counter changes received from the GGSN. See details in the Operator Notes.
- New command sets the variance allowed between values for received restart counter changes.
- New command sets the rate of PDP deactivations due to GTP-C path failures.
- New command disables the new default verification behavior.

Network Overload Protection - Optimized

The SGSN's optimized network overload protection performs attach-rate throttling to avoid overloading Gr, Gn and Gf interfaces. When enabled, the IMSIMgr throttles the attach rate to a value configured with a new set of *queue-size* and *wait-time* keywords.

If the SGSN receives more than the configured number of attaches in a second, then the attaches are buffered in the pacing queue and requests are only dropped when the buffer overflows due to high incoming attach rate. Messages in the queue are processed (FIFO) until they age-out when the queued message's lifetime crosses the configured wait-time. The wait-time and the attach rate decide the optimal size of the queue.

Paging for Packets Queued in the BSSGP Layer - Behavioral Change

Previous Behavior: If an MS became unreachable or moved into Stand-by, the state of the MS was marked as 'suspended' in the BSSGP layer. The SGSN did not initiate Paging so packets for that MS remained in the BSSGP BVC/MS flow control queue until the SGSN received an uplink packet or a new packet for the MS from the GGSN.

New Behavior: Now if the SGSN becomes aware that the MS moves to standby state, due to expiry of the ready timer or due to radio status, the SGSN initiates PS-Paging towards the MS. If the MS responds to the Paging, then the SGSN can resume sending queued packets without waiting for any activity from/for the MS. This results in a reduction of unnecessary queuing of data.

Printing Format Changed for RAI and OLD-RAI Fields - Behavioral Change

The GMM-SM event logging feature has been enhanced so that the EDR print format is no longer fixed in length. The length is now variable. So, if the MNC has 2 digits then the RAI or OLD-RAI print format does not append a zero “0” which could cause an MNC error. During the GMM-SM event logging, the RAI and OLD-RAI fields in the EDR now have a variable length depending on the number of digits in the MNC. Based on the MNC, the length can now be 15 (xxx-xxx-xxxx-xx) or 14 (xxx-xx-xxxx-xx) characters. For example, if MNC has 2 digits “09” then the RAI or OLD_RAI prints as - xxx-09-xxxx-xx.

P-TMSI Signature Validation Feature

When enabled, this feature allows the SGSN to send the Attach Reject for the Attach Request received with a P-TMSI signature mismatch message. This is done, primarily, to avoid the identification of incorrect mapping of P-TMSI/IMSI at the SGSN if the P-TMSI was allocated to a different MS. Enabling this feature allows the SGSN to validate the PTMSI signature present in the Attach Request against the PTMSI-SIGNATURE stored in the SGSN and then the SGSN sends the Attach Reject to the MS if the P-TMSI signature does not match.

This is applicable only for 2G attaches and this configuration forces the operator to enable P-TMSI reallocation during Attach and INTER-SGSN-RAU procedures.

PSC3 Card Qualified for SGSN

The SGSN now supports the PSC3 ***limited to PSC2-level capacity***. This means the PSC3 in an SGSN currently supports the same number of subscribers as the SGSN with PSC2 cards. No special configuration is required.

Selective Authentication/P-TMSI Reallocation/ P-TMSI Signature Reallocation - Behavioral Change

Previous Behavior: Subscriber event authentication, P-TMSI reallocation and P-TMSI signature reallocation were default functions.

New Behavior: Authentication for Attach Request, Activate Request, Service Request, RAU Request, SMS Request, and Detach Request is now performed selectively and requires operator configuration to enable the functionality. Authentication and P-TMSI reallocation enabling configuration are only applicable when the SGSN’s performance of these functions is optional.

The command structures of the subscriber event authentication, and of the P-TMSI reallocation and P-TMSI signature reallocation have been re-architected to ensure a consistent and more intuitive user experience. As a result, there are now three consistent forms for each command. The functionality is now selective and the configuration forms of the commands now enable the functionality optionally for:

- Every instance or every nth instance of a procedure
- On the basis of UMTS or GPRS or both
- On the basis of elapsed time intervals between events.

The ‘no’ forms of the commands consistently disable the functionality in the configuration file. The ‘remove’ forms of the commands consistently delete the specified functionality from the call control profile configuration. As these functions are now performed selectively, according to the operator’s configuration in a call control profile, all default forms of these commands have been deprecated.

Authentication and P-TMSI reallocation enabling configurations are only applicable when the SGSN’s performance of these functions is optional.

There are situations in which authentication will be performed unconditionally:

- IMSI Attach – all IMSI attaches will be authenticated
- When the subscriber has not been authenticated before and the SGSN does not have a vector
- When there is a P-TMSI signature mismatch
- When there is a CKSN mismatch

There are situations in which P-TMSI will be reallocated unconditionally:

- Inter SGSN Attach/RAU
- Inter-RAT Attach/RAU in 2G
- IMSI Attach

Threshold for Additional Authentication Vectors

The software has been enhanced to allow the operator to configure a threshold indicating the minimum number of unused vectors that should be maintained by the SGSN before it initiates a SAI to refill the buffer. With this feature enabled, the SGSN will maintain a specific number of unused vectors at all times. The SAI is initiated when a vector is used up by the SGSN for authentication and the configuration threshold is hit. The SAI initiated, due to this configuration, will be ongoing in parallel to the procedures. This feature changes how many vectors are retrieved from the HLR each time and stored on the SGSN so it should increase performance by decreasing the amount of interaction with the HLR during procedures.

TPO Optimization on the GGSN

To reduce the impact of handoffs on TCP flows, optimizations (traffic performance optimization – TPO) will be done at the GGSN. The GGSN needs to be made aware of handoffs before handoffs are completed to reduce the interruptions on the data plane.

The old SGSN informs the GGSN about the start of handoff through a self-generated GTPU packet with proprietary private extensions. The GGSN does not treat this packet as an uplink packet but as an indication that handoff is going to occur. The SGSN sends a pre-handoff GTPU notification to a GGSN only if the GGSN has sent a proprietary GTPU message to inform the SGSN of the GGSN's interest in knowing about handoffs. The SGSN does not treat this GTPU message as a downlink packet.

NOTE: This solution works ONLY between ASR 5000 SGSNs running release 12.2 and ASR 5000 GGSNs running release 12.2. This feature is configured and initiated at the GGSN.

Unlimited Zone Code Lists - Behavioral Change

Previous behavior: Previously, it was only possible to configure up to 10 zone code lists per Call Control Profile.

New Behavior: The assignment of zone codes has been altered. There is no longer a limit to the number of zone code lists that can be configured per Call Control Profile because the zone code lists are now dynamically allocated based on configuration.

The SGSN zone code lists are configured with the zone-code command in the call control profile configuration mode to create a zone code which lists one or more location areas (LACs) into which a subscriber is allowed to roam. Previously, there was a static limit of 10 zone codes configurable per call control profile. The subscriber may need more flexibility than 10 zone codes per call control profile, however, it is impossible to predict the maximum number required. So the implementation has changed from a static number of zone codes configured per call control profile to an unlimited number utilizing dynamically allocated memory for zone codes defined for call control profiles.

Update GPRS Location (UGL) Logic Enhancements

The handling of subscription data in the SGSN database has been modified as follows:

- SGSN sends a UGL on a Routing Area Update (RAU)/ Attach Request from an area which is served by a different SGSN number/MAP service/SGTP service. All fallbacks from various services are handled gracefully
- SGSN sends a Purge to the HLR on subscriber cleanup whenever a successful UGL is done.
- SGSN sends a UGL upon uplink activity after an HLR reset. Interaction with the next Attach/RAU as uplink activity should then be handled correctly

Forcing Authentication when MS/UE Security Fails

When GMM authentication is skipped, the SGSN and the MS continue to re-use the latest keys exchanged during the most recent GMM authentication procedure. This can result in

the SGSN and the MS going out of sync with the CK and IK currently in use. If a mismatch occurs, then the security mode can timeout or be rejected because the MS will not be able to decipher or perform integrity checks on network messages. This can introduce useless signaling in the network.

This feature allows the operator to enable a forced GMM authentication that will either resolve this type of problem or avoid it. As well, operators can configure a frequency of authentication that best meets their needs.

Subscriber Service Controller in Release 12.1

Subscriber Service Controller (SSC) is an application that complements and extends the functionality of Intelligent Policy Control Function (IPCF).

SSC uses Subscriber Profile Repository (SPR) data store, to implement the usage control policies in a centralized manner. It also handles account details as well as session state information of the subscriber. SSC can manage the event notification function for PCC, by sending e-mails or text messages to subscribers. SSC provides storage facility for subscriber profile along with centralized management of subscriber policy and quota for your deployment. SSC works in conjunction with IPCF, PPT and other PCC components

Release 12.1 supports following features

Bulk Load Provisioning Support

Subscriber profiles need to be available in SSC, so that IPCF can process policy rules based on these profiles.

To enable the subscriber specific policy control, such profile information needs to be loaded in bulk into the SSC database, from the legacy database. SSC provides a mechanism to bulk load the data related to subscriber profile, provided that such data is stored in the specified Comma Separated Value (CSV) format. The source data file is stored as external table in the database, the BulkLoad_sub script executes SQL statements that load actual data into database tables. This script can be scheduled to execute during the low activity period.

Event Notification Management

SSC uses event notification module to provide usage and policy notifications to the subscriber.

These notifications are mostly related with subscriber's service usage scenario or policy changes imposed by PCC rules that might affect subscriber. SSC generates this information by exchanging subscriber profile as well as usage information with other components of PCC solution such as IPCF or PPT as well as with OSS and BSS systems.

SSC event notification module receives change triggers from service usage as well as policy management modules of IPCF. Change triggers are the events on whose execution, notifications are sent to subscribers regarding changes in their service usage or profile status. Notifications can be sent as an SMS or e-mail using subscriber's Mobile Subscriber ISDN Number (MSISDN) or registered e-mail id.

Usage Monitoring Functions

SSC acts as a centralized repository for data pertaining to subscriber profile, policy and service usage.

As per your network configuration and business model, you can configure SSC to exchange this data between IPCF and various Operation Support Systems (OSS) as well as Billing Support Systems (BSS). Thus extending the data monitoring capacity of IPCF. OSS software applications are used to administer operational processes related to network infrastructure and services such as QoS monitoring, network and server performance. OSS applications also provide logical or element and physical or network management of the deployed resources. Provisioning function can also be handled by OSS applications. BSS software applications are used to administer external business operations such as billing, rating, sales or customer management. BSS application can also be used to administer customer databases.

SSC Bulk Statistics Support

SSC provides a bulk statistics framework which can be used to record various system related statistics such as counters, gauges and fixed value strings from various SSC schema of your deployment.

This framework can be used for recording as well as monitoring of such bulk statistics.Statistical counters provide a snapshot of the system at any given instant.The bulk statistics collected over a regular and configurable time interval can be used for administering SSC deployment as well as for troubleshooting purpose. User can compare values of such counters on a discrete time line specified by the sampling period, to diagnose the system health.

SSC Application High Availability in Multi Host Cluster Deployment

High Availability (HA) feature is implemented for a multi-host SSC cluster deployment.

This feature ensures availability of application and management interfaces of SSC in case of a catastrophic event at any of the SSC nodes. These interfaces are used by SSC to exchange data with other components of PCC solution such as IPCF,PPT and OSS or BSS. If an SSC node supporting any of these interfaces fails, then the HA feature allows initialization of supported interfaces from one of the remaining nodes in the SSC cluster.

SSC Real Application Cluster (RAC) Support

Enhanced SSC architecture supports Oracle Real Application Cluster (RAC).

The RAC allows Oracle data base to run any packaged or custom application un-changed across the server pool. It provides facility to add more servers and instances to the pool without taking the users offline. In the previous SSC architecture, the data base can become single point of failure as well as performance bottle neck as it is installed on a single blade in any site. With RAC, Oracle de-couples the Oracle instance i.e. the processes and memory structures that are running on the server to access the data, from the data files i.e. the physical structure that is actually storing the data. A clustered database can be accessed by multiple instances running on separate servers.

For information about the SSC, refer *Subscriber Service Controller Installation and Administration Guide.*

Web Element Manager Features in Release 12.0

This section provides information for new features for the Web Element Manager (WEM) application in Release 12.0.

Cisco MITG RHEL v5.5 OS Support for WEM

The Web Element Manager is now supported on selected Cisco UCS servers running the custom Cisco MITG Red Hat Enterprise Linux (RHEL) v5.5 operating system (OS).

For detailed hardware platform and hard disk drive partition requirements, refer to the *Web Element Manager Overview* chapter of the *Cisco Web Element Manager Installation and Configuration Guide*. For installation information, refer to the *Cisco MITG RHEL v5.5 OS Application Note*.

IMPORTANT

The Cisco MITG RHEL v5.5 OS is a custom image that contains only those software packages required to support compatible Cisco MITG external software applications. Users must not install any other applications on servers running the Cisco MITG v5.5 OS. For detailed software compatibility information, refer to the *Cisco MITG RHEL v5.5 OS Application Note.*

Redundant Server Support Using Cluster Software

Previously with WEM configured as single installations, there was a Single Point of Failure (SPoF).

Multiple WEM servers can now be configured as part of a redundant High Availability failover cluster.

Oracle Cluster software is supported on Sun servers with the Solaris operating system.

Symantec Veritas Cluster software is supported on both Sun servers using Solaris or RHEL operating system and Cisco UCS servers using RHEL.

Refer to the appendices in the *Cisco Web Element Manager Installation and Administration Guide* for detailed configuration information.

Support for Disabling FTP ESPV Mode in *bsserver.cfg* File

WEM users now have the option to disable Extended Passive (EPSV) Mode for FTP file transfers of bulk statistic information. By default, WEM uses EPSV mode. To disable ESPV mode, set the FTP_USE_EPSV= field in the WEM server's *bsserver.cfg* file to **0**.

Support for Femto Protocols in Monitor Protocol/Subscriber

WEM now supports the monitoring of protocols and subscribers via the HNBAP and RUA Femto protocols.

Web Element Manager Path

- Monitor/Test | Monitoring Operations | Monitor Protocol
- Monitor/Test | Monitoring Operations | Monitor Subscriber

Chassis Name Included in License Update Message

When a license update operation is performed in the Exec Mode Commands screen, the license update message now specifies the name of the chassis for which the license was updated.

Web Element Manager Path

Performance | Exec Mode Commands

Removal of migrate.tar.gz File

The migrate.tar.gz file, which provided files that performed WEM database backup and restore functions, has been removed as a separate.tar.gz file from the WEM installation package. Instead, the files related to WEM database and restore functionality now are extracted as individual files when the WEM installation .tar file is unzipped. The files include:

- ems_migrate
- ems_migrate.cfg
- README.ems_migrate

Enhancement to WEM Installation Script on RHEL Platform

The WEM installation script for Red Hat Linux platforms now automatically sets the core file size for the WEM installation to *unlimited*. This eliminates the need for users to manually set this parameter.

To view the core file size (blocks) setting, navigate to the *<ems_dir_name>/server* directory on the UCS RHEL server and enter the **`./serv`** status command.

Solaris Patch Upgrade for U.S.Time Zone

Users based in the United States should ensure that the timezone patch 113225-07 (or later) and libc patch 112874-33 (or later) be installed in support of extended daylight savings time (DST) support.

In addition, if Solaris 9 is used, it must be installed using the “End User System support 64-bit” software group must be specified during the installation of the operating system. This option installs the libraries required for proper operation of the Web Element Manager.

For United States users of Solaris 10 with a Recommended Patch Cluster dated on or after April 2011: Users with Solaris 10 should ensure that the timezone patch 138856-02 or later is installed in support of extended Daylight Savings Time (DST).

Hide or Display Option for GUI Pull-Down Menus and Sub-Menus

Administrators have the ability to hide or display any parent menu and submenu in the GUI as required. This allows the Admin to control what is or is not accessible to the WEM user.

This is controlled by a flag set in the *menu.xml* file. This file, and an example of how to set the flag, are described in the "Configuration File" appendix in the *Cisco WEM Installation and Administration Guide*. It is also described in a Read Me in the Online Help files.

Improved Support for Solaris Installations with New Patch Advisory

Certain patches from Solaris had shown themselves to be unstable There are improvements in stability by installing the following new Patches, documented in the *Overview* section of the *Web Element Manager Installation and Administration Guide:*

The following changes are suggested:

Solaris 10 with Recommended Patch Cluster dated on or after July 16, 2007 and not later than Nov 2010. Do **not** install the kernel patch beyond 142900-07.

IMPORTANT: Solaris 10 Kernel patch released between 137137-09 and 142900-04 may result in kernel panic while executing/invoking system calls. Solaris 10 Kernel patch released after 142900-07 has an issue, which will result in failure while invoking WEM Monitor subscriber and Monitor protocol screens.

Support for Auto Discovery of New Chassis

Previously the Auto Discovery Dialog Box did not discriminate between newly found devices and devices that had been in the database for an indeterminate amount of time, leading to administrative confusion and the possibility of duplication in the database.

The Auto Discovery Dialog Box now supports a new feature where if a discovery is started, only chassis discovered during the latest sweep will be added to the Discovery Result area. If any device discovered during this sweep is already in the database, then a checkbox in the IMGList Added column will be checked. This will prevent the Admin trying to add it twice. If all chassis found during this search have already been added to the database, then all entries will have the checkmark and the **Add to IMGList** button will be disabled.

For any newly discovered chassis without a checkmark, the Admin can add it to the database using the **Add to IMGList** button.

Any chassis discovered prior to the current search and already in the database is ignored.

The WEM path is Monitor Test Menu | Monitor Operations | Auto Discovery

Installation Fails on RHEL O/S with Various X11 Error Messages

Previously, installations on the RHEL O/S would fail with error messages such as "X connection to localhost:10.0 broken (explicit kill or server shutdown)."

Workarounds to solve this problem by enabling X11 Forwarding are documented in the *Troubleshooting* chapter of the *Web Element Manager Installation and Administration Guide*

Filter Created to Display Subsets of All WEM Users: Inactive or Never Logged In

A new filter has been created because administrators found it difficult to check which users were actually logged in, or had never logged in.

The "Inactive / User Never Logged In" check box has been added to the “Search On” panel in the WEM Users tab on the User Administration screen.

When this checkbox is selected either the Inactive or the User Never Logged In radio button can be selected to filter just those users.

If this checkbox is not selected all users would be displayed.

The WEM path is Security | User Administration.

Web Element Manager Features in Release 12.2

There following are new features for the Web Element Manager (WEM) application in Release 12.2.

WEM, MUR, InTracer and PPT Co-Located on One Server

Web Element Manager, MUR, PPT and InTracer software can now be co-located on a Cisco UCS server running Cisco MITG RHEL Operating System. This is documented in the *MITG RHEL Application Note*.

There is a caveat that because WEM and MUR are both processor-intensive, running both on the same server is not recommended.

Improved Support for Solaris Installations with New Patch Advisory

Certain patches from Solaris had shown themselves to be unstable There are improvements in stability by installing the following new Patches, documented in the *Overview* section of the *Web Element Manager Installation and Administration Guide:*

The following changes are suggested:

Solaris 10 with Recommended Patch Cluster dated on or after July 16, 2007 and not later than November 2010. Do **not** install the kernel patch beyond 142900-07.

IMPORTANT: Solaris 10 Kernel patch released between 137137-09 and 142900-04 may result in kernel panic while executing/invoking system calls. Solaris 10 Kernel patch released after 142900-07 has an issue, which will result in failure while invoking WEM Monitor Subscriber and Monitor Protocol screens.

Superuser Password Change Required on Next Login

If the superuser password is reset using the script *./set_superuser_password.sh,* then on the next login the user is prompted to change the password as the password “superuser” is temporary and does not conform to password strength requirements. After the change, the user can login with the new password.

For further information on *./set_superuser_password.sh* configuration, refer to the *Cisco Web Element Manager Installation and Administration Guide.*

MITG-RHEL Application Note Change

The note concerning X-11 configuration has been removed.

New Pending Alarm View Menu Option

Previous Behavior: There was no Pending Alarm View

Modified Behavior: A new screen for Pending Alarm View has been added to the Alarm menu in WEM that includes an optional date filter.

If the filter is used, the available date options are:

- Last Month
- Last 7 days
- Yesterday
- Today
- Specific Date Range

WEM Online Help path to this screen is Alarm Menu\Pending Alarm View\Dialog Boxes\Set Pending Alarm Filter.

Script for Upgrading Non-Database WEM Tables in Cluster Mode

During a WEM upgrade in cluster mode, the WEM now automatically executes a script that will upgrade all non-database WEM tables. A README file is included with the WEM installer package that provides details about the script's functionality.

High Availability Redundant Clustering Not Supported on Solaris

Support for configuring redundant WEM servers using Oracle Cluster Software has been withdrawn. Redundant WEM server configuration is now supported using Veritas Cluster Software from Symantec on Cisco UCS servers using the MITG-RHEL O/S.

The *Cisco Web Element Manager Installation and Administration Guide* is undergoing review.

CHAPTER 2
FAULT MANAGEMENT

This chapter identifies additions and changes made to fault management features in Release 12.0, 12.1, and 12.2.

Topics covered in this chapter are:

SNMP MIB Objects and Alarms

This section lists additions and changes to MIB objects and alarms in Release 12.x.

SNMP MIB Objects and Alarms in Release 12.0

This section lists additions and changes to MIB objects and alarms in Release 12.0.

Omissions and Corrections to Past Releases

During a review of the *Cisco ASR 5000 SNMP MIB Reference*, it was discovered that the external management applications had been documented with Object ID strings that were inconsistent with the MIB files present in the software. This affects all releases up to and including 10/31/2012.

In order to correct this, a new hierarchy diagram has been created for each product, and the OID strings have been corrected in the most current user documentation, released 11/30/2012.

This correction is NOT required for the starOS MIB objects; however, a new hierarchy diagram has been added for clarity.

The following table defines the changes for the MIB Objects OID strings. The OID strings continue to be prefaced with “enterprise” to represent 1.3.6.1.4.1:

Application	Previously Documented OID String	Corrected OID String
Content Filtering supports multiple MIBs:		
starCFCommonMIB	enterprise.8164.1.100.1.1.*x*	enterprise.8164.100.1.1.*x*
starCFCDPMIB	enterprise.8164.1.100.2.1.*x*	enterprise.8164.100.2.1.*x*
starCFREMIB	enterprise.8164.1.100.3.1.*x*	enterprise.8164.100.3.1.*x*
starCFCCIMIB	enterprise.8164.1.100.4.1.*x*	enterprise.8164.100.4.1.*x*

Application	Previously Documented OID String	Corrected OID String
starCFEMSMIB		*enterprise.8164.100.5.1.*x*
*enterprise.8164.100.5.1.*x* has been added as a placeholder for possible future development		
starCFMCRDBSMIB	enterprise.8164.1.100.6.1.*x*	enterprise.8164.100.6.1.*x*
IPMS	enterprise.8164.1.102.1.*x*	enterprise.8164.102.1.*x*
MUR	enterprise.8164.1.103.1.*x*	enterprise.8164.103.1.*x*
PPT	enterprise.8164.1.104.1.*x*	enterprise.8164.104.1.*x*
SSC	enterprise.8164.1.201.1.*x*	enterprise.8164.201.1.*x*
WEM	enterprise.8164.1.1000.1.*x*	**enterprise.8164.1.1000.1.*2.x*
**Note that WEM retains the “1” after 8164 and adds “2” to the string		

The following table defines the changes for the MIB Traps OID strings. The OID strings continue to be prefaced with “enterprise” to represent 1.3.6.1.4.1:

Application	Previously Documented OID String	Corrected OID String
Content Filtering supports multiple MIBs:		
starCFCommonMIB	enterprise.8164.1.100.1.1.*x*	enterprise.8164.100.1.1.*x*
starCFCDPMIB	enterprise.8164.1.100.2.1.*x*	enterprise.8164.100.2.1.*x*
starCFREMIB	enterprise.8164.1.100.3.1.*x*	enterprise.8164.100.3.1.*x*
starCFCCIMIB	enterprise.8164.1.100.4.1.*x*	enterprise.8164.100.4.1.*x*
starCFEMSMIB		*enterprise.8164.100.5.1.*x*
*enterprise.8164.100.5.1.*x* has been added as a placeholder for possible future development		
starCFMCRDBSMIB	enterprise.8164.1.100.6.1.*x*	enterprise.8164.100.6.1.*x*
IPMS	enterprise.8164.1.102.1.*x*	enterprise.8164.102.1.*x*
MUR	enterprise.8164.1.103.1.*x*	enterprise.8164.103.1.*x*
PPT	enterprise.9.1.787.1.*x*	enterprise.9.9.787.0.*x*
SSC	enterprise.8164.1.201.1.*x*	enterprise.8164.201.1.*x*
WEM	enterprise.8164.1.1000.1.*x*	**enterprise.8164.1.1000.1.*2.x*
**Note that WEM retains the “1” after 8164 and adds “2” to the string		

The following table defines the changes for the MIB Conformances OID strings. The OID strings continue to be prefaced with “enterprise” to represent 1.3.6.1.4.1:

The most common finding was that MIBGroups and MIBCompliances OID strings were reversed in some cases. Although not all applications were affected, the following is the correct OID string for *all* applications, corrected as per the MIB file, as reflected in the most current user documentation of 11/30/2012:

Application	OID String
starCFCommonMIB	Possible future development
starCFCDPMIB	Possible future development
starCFREMIB	enterprise.8164.100.3.3.starCFREMIBGroups(1).x enterprise.8164.100.3.3.starCFREMIBCompliances(2).x
starCFCCIMIB	enterprise.8164.100.4.3.starCFCCIMIBGroups(1).x enterprise.8164.100.4.3.starCFCCIMIBCompliances(2).x
starCFEMSMIB	Possible future development
starCFMCRDBSMIB	enterprise.8164.100.6.3.starCFMCRDBSMIBGroups(1).x enterprise.8164.100.6.3.starCFMCRDBSMIBCompliances(2).x
starEMSMIB (WEM)	enterprise.8164.1.1000.3.starEmsMIBCompliances(1).x enterprise.8164.1.1000.3.starEmsMIBGroups(2).x
starIPMSMIB	enterprise.8164.102.3.starIPMSMIBCompliances(1).x enterprise.8164.102.3.starIPMSMIBGroups(2).x
starMURMIB	enterprise.8164.103.3.starMURMIBGroups(1).x enterprise.8164.103.3.starMURMIBCompliances(2).x
starPPTMIB	enterprise.8164.104.3.starPPTMIBGroups(1).x enterprise.8164.104.3.starPPTMIBCompliances(2).x
starSSCMIB	enterprise.8164.201.3.starSSCMIBGroups(1).x enterprise.8164.201.3.starSSCMIBCompliances(2).x
For the WEM application, see starEMSMIB	

New Objects

- starMVGEndpointName
- starMVGCauseCode
- starThreshEPDGCurrSess
- starThreshClearEPDGCurrSess
- starThreshSystemCapacity
- starThreshClearSystemCapacity
- starThreshCPUUtilization
- starThreshClearCPUUtilization
- starApsCommandSuccess
- starApsCommandFailure
- starApsSwitchSuccess
- starApsSwitchFailure

- starApsModeMismatch
- starApsChannelMismatch
- starApsByteMismatch
- starApsFeProtLineFailure
- starApsLossOfRedundancy
- starApsLossOfRedundancyClear
- starEmsBulkStatFilterDetails
- starEmsBulkStatCurrentDouble
- starEmsBulkStatThresholdDouble
- starEmsConfigBackupFileName
- starEmsConfigBackupFtpFailed
- starEmsConfigBackupFtpSuccess
- starEmsBulkStatIncrementalCounterThresholdAboveLimit
- starEmsBulkStatIncrementalCounterThresholdNormal
- starEmsBulkStatGaugeCounterUsageOverLimit
- starEmsBulkStatGaugeCounterUsageNormal
- starEmsConfigBackupFileDiff
- starMURThreshComaparator
- starMURKPITable
- starMURKPIEntry
- starMURGatewayName
- starMURKPIName
- starMUREntityName
- starMURThreshConfiguredString
- starMURThreshMeasuredString
- starMURKPIThreshCritical
- starMURKPIThreshCriticalClear
- starMURKPIThreshMajor
- starMURKPIThreshMajorClear
- starMURKPIThreshMinor
- starMURKPIThreshMinorClear
- starMURKPIThreshWarning
- starMURKPIThreshWarningClear
- starSGSServiceStart
- starSGSServiceStop
- starSgsnGnMsgDelay
- starSgsnGnMsgDelayClear
- starENBID

- starThreshPCCPolicySessions,
- starThreshClearPCCPolicySessions,
- starThreshPerServicePCCPolicySessions,
- starThreshClearPerServicePCCPolicySessions,
- starThreshPCCQuotaSessions,
- starThreshClearPCCQuotaSessions,
- starThreshPerServicePCCQuotaSessions,
- starThreshClearPerServicePCCQuotaSessions,
- starThreshPCCAFSessions,
- starThreshClearPCCAFSessions
- starThreshPerServicePCCAFSessions
- starThreshClearPerServicePCCAFSessions

Modified Objects

- starPCFRrqRcvd
- starPCFRrqAccepted
- starPCFRrqDenied
- starPCFRrqDiscarded
- starPCFInitialRrqRcvd
- starPCFInitialRrqAccepted
- starPCFIntraPDSNActiveHORrqAccepted
- starPCFIntraPDSNDormantHORrqAccepted
- starPCFInterPDSNHORrqAccepted
- starPCFInitialRrqDenied
- starPCFInitialRrqDiscarded
- starPCFRenewRrqRcvd
- starPCFRenewRrqAccepted
- starPCFRenewActiveRrqAccepted
- starPCFRenewDormantRrqAccepted
- starPCFRenewRrqDenied
- starPCFRenewRrqDiscarded
- starPCFDeregRrqRcvd
- starPCFDeregRrqAccepted
- starPCFDeregDormantRrqAccepted
- starPCFDeregRrqDenied
- starPCFDeregRrqDiscarded
- starPCFIntraPDSNActiveAnidHORrqAccepted
- starPCFIntraPDSNDormantAnidHORrqAccepted
- starPCFDeniedUnSpeReason

- starPCFDeniedUnSpeReason
- starPCFDeniedInsufResource
- starPCFDeniedMobNodeAuthFail
- starPCFDeniedIdentMismatch
- starPCFDeniedPoorFormedReq
- starPCFDeniedUnknownPDSNAddr
- starPCFDeniedRevTunnelUnavail
- starPCFDeniedRevTunnelRequire
- starPCFDeniedUnrecogVendorId
- starPCFDeniedSessionClosed
- starPCFDeniedBsnSessionInfoUnavail
- starPCFRegUpdTransmitted
- starPCFRegUpdAccepted
- starPCFRegUpdateRpLifetimeExpiry
- starPCFRegUpdateUpperLayerIntiated
- starPCFRegUpdateOtherReason
- starPCFRegUpdateHORelease
- starPCFRegUpdateSessmgrDied
- starPCFAuxA10ConnectionsSetup
- starPCFSessionsDenied
- starPCFSessionsInit
- starPCFSessionsReneg
- starPCFDiscLcpRemote
- starPCFDiscRpRemote
- starPCFDiscRpLocal
- starPCFDiscMaxIpcpRetr
- starPCFDiscMaxIpv6cpRetr
- starPCFDiscMaxLcpRetr
- starPCFDiscAuthFail
- starPCFDiscSessSetupTimeout
- starPCFDiscFlowAddFail
- starPCFDiscInvDestContext
- starPCFDiscLcpOptFail
- starPCFDiscIpcpOptFail
- starPCFDiscIpv6cpOptFail
- starPCFDiscNoRemIpAddr
- starPCFDiscDetectionFail
- starPCFDiscMisc

- starPCFCurrentSessions
- starPCFSessionsSetup
- starPCFSessionsRelsese
- starPCFCurrentRevaSessions
- starEmsBulkStatThreshold
- starEmsBulkStatCurrent
- starEmsBulkStatCounterThresholdAboveLimit
- starEmsBulkStatCounterThresholdNormal
- starEmsBulkStatCounterUsageOverLimit
- starEmsBulkStatCounterUsageNormal
- starEmsNotifMgmtGroup
- starEmsNotifGroup
- starMURNotifMgmtGroup
- starPCFRrqRcvd
- StarentCardType

- has added support for the following hardware Enumerations:

- pscA(24) -- Packet Services Card A
- ppc(25) -- Packet Processing Card
- lcchan3p2(26) -- Channelized Line card 2 Port
- lcchan3p4(27) -- Channelized Line card 4 Port
- fanctrl6(28) -- Fan control revision 6
- vioc(29) -- Virtual I/O Card
- gpdsp(30) -- GP-DSP Daughter Card
- xme(31), --XME Daughter Card
- vop(32) -- VOP Daughter Card
- edc(33)

Obsoleted Objects

None for this release.

New Alarms

- starSGSNRNCNoResetAck

Modified Alarms

- starAAAArchiveStarted has a modified description.

For October 30, 2012:

The following traps all added a new Object: starSS7M3UACauseStr. The Arguments also changed as noted:

- starM3UAPCUnavailable; arguments now {0,1,2,3}

- starM3UAPCAvailable; arguments now {0,1,2,3}
- starM3UAPSPDown; arguments now {0,1,2,3}
- starM3UAPSPUp; arguments now {0,1,2,3}
- starSCTPPathDown {0,1,2,3,4,5,6,7}
- starSCTPPathUp {0,1,2,3,4,5,6,7}

The following traps added new Objects: starSS7CongLevel and starSS7LocalCong. The arguments also changed as noted:

- starSS7PCCongested; arguments now {0,1,2,3}
- starSS7PCCongestionCleared; arguments now {0,1,2,3}

The following traps added new Object: starSS7CongLevel.

- starM3UAPSPCongested
- starM3UAPSPCongestionCleared

Obsoleted Alarms

None for this release.

Web Element Manager Path

Select Configuration | SNMP Configuration.

SNMP MIB Objects and Alarms in Release 12.1

This section lists additions and changes to MIB objects and alarms in Release 12.1.

Omissions and Corrections to Past Releases

During a review of the *Cisco ASR 5000 SNMP MIB Reference*, it was discovered that the external management applications had been documented with Object ID strings that were inconsistent with the MIB files present in the software. This affects all releases up to and including 10/31/2012.

In order to correct this, a new hierarchy diagram has been created for each product, and the OID strings have been corrected in the most current user documentation, released 11/30/2012.

This correction is NOT required for the starOS MIB objects; however, a new hierarchy diagram has been added for clarity.

The following table defines the changes for the MIB Objects OID strings. The OID strings continue to be prefaced with “enterprise” to represent 1.3.6.1.4.1:

Application	Previously Documented OID String	Corrected OID String
Content Filtering supports multiple MIBs:		
starCFCommonMIB	enterprise.8164.1.100.1.1.*x*	enterprise.8164.100.1.1.*x*
starCFCDPMIB	enterprise.8164.1.100.2.1.*x*	enterprise.8164.100.2.1.*x*
starCFREMIB	enterprise.8164.1.100.3.1.*x*	enterprise.8164.100.3.1.*x*
starCFCCIMIB	enterprise.8164.1.100.4.1.*x*	enterprise.8164.100.4.1.*x*
starCFEMSMIB		*enterprise.8164.100.5.1.*x*
*enterprise.8164.100.5.1.*x* has been added as a placeholder for possible future development		
starCFMCRDBSMIB	enterprise.8164.1.100.6.1.*x*	enterprise.8164.100.6.1.*x*
IPMS	enterprise.8164.1.102.1.*x*	enterprise.8164.102.1.*x*
MUR	enterprise.8164.1.103.1.*x*	enterprise.8164.103.1.*x*
PPT	enterprise.8164.1.104.1.*x*	enterprise.8164.104.1.*x*
SSC	enterprise.8164.1.201.1.*x*	enterprise.8164.201.1.*x*
WEM	enterprise.8164.1.1000.1.*x*	**enterprise.8164.1.1000.1.*2*.*x*
**Note that WEM retains the “1” after 8164 and adds “2” to the string		

The following table defines the changes for the MIB Traps OID strings. The OID strings continue to be prefaced with “enterprise” to represent 1.3.6.1.4.1:

Application	Previously Documented OID String	Corrected OID String
Content Filtering supports multiple MIBs:		
starCFCommonMIB	enterprise.8164.1.100.1.1.*x*	enterprise.8164.100.1.1.*x*
starCFCDPMIB	enterprise.8164.1.100.2.1.*x*	enterprise.8164.100.2.1.*x*
starCFREMIB	enterprise.8164.1.100.3.1.*x*	enterprise.8164.100.3.1.*x*
starCFCCIMIB	enterprise.8164.1.100.4.1.*x*	enterprise.8164.100.4.1.*x*
starCFEMSMIB		*enterprise.8164.100.5.1.*x*
*enterprise.8164.100.5.1.*x* has been added as a placeholder for possible future development		
starCFMCRDBSMIB	enterprise.8164.1.100.6.1.*x*	enterprise.8164.100.6.1.*x*

Application	Previously Documented OID String	Corrected OID String
IPMS	enterprise.8164.1.102.1.*x*	enterprise.8164.102.1.*x*
MUR	enterprise.8164.1.103.1.*x*	enterprise.8164.103.1.*x*
PPT	enterprise.9.1.787.1.*x*	enterprise.9.9.787.0.*x*
SSC	enterprise.8164.1.201.1.*x*	enterprise.8164.201.1.*x*
WEM	enterprise.8164.1.1000.1.*x*	**enterprise.8164.1.1000.1.*2*.*x*
**Note that WEM retains the “1” after 8164 and adds “2” to the string		

The following table defines the changes for the MIB Conformances OID strings. The OID strings continue to be prefaced with “enterprise” to represent 1.3.6.1.4.1:

The most common finding was that MIBGroups and MIB Compliances OID strings were reversed in some cases. Although not all applications were affected, the following is the correct OID string for *all* applications, corrected as per the MIB file, as reflected in the most current user documentation of 11/30/2012:

Application	OID String
starCFCommonMIB	Possible future development
starCFCDPMIB	Possible future development
starCFREMIB	enterprise.8164.100.3.3.starCFREMIBGroups(1).x enterprise.8164.100.3.3.starCFREMIBCompliances(2).x
starCFCCIMIB	enterprise.8164.100.4.3.starCFCCIMIBGroups(1).x enterprise.8164.100.4.3.starCFCCIMIBCompliances(2).x
starCFEMSMIB	Possible future development
starCFMCRDBSMIB	enterprise.8164.100.6.3.starCFMCRDBSMIBGroups(1).x enterprise.8164.100.6.3.starCFMCRDBSMIBCompliances(2).x
starEMSMIB (WEM)	enterprise.8164.1.1000.3.starEmsMIBCompliances(1).x enterprise.8164.1.1000.3.starEmsMIBGroups(2).x
starIPMSMIB	enterprise.8164.102.3.starIPMSMIBCompliances(1).x enterprise.8164.102.3.starIPMSMIBGroups(2).x
starMURMIB	enterprise.8164.103.3.starMURMIBGroups(1).x enterprise.8164.103.3.starMURMIBCompliances(2).x
starPPTMIB	enterprise.8164.104.3.starPPTMIBGroups(1).x enterprise.8164.104.3.starPPTMIBCompliances(2).x
starSSCMIB	enterprise.8164.201.3.starSSCMIBGroups(1).x enterprise.8164.201.3.starSSCMIBCompliances(2).x
For the WEM application, see starEMSMIB	

It was found that a number of new traps had been mis-identified as modified objects when in reality they are new traps. They have been moved to the New Traps section:

- starSSCProcessStartFail
- starSSCFTPServerUnreachable
- starSSCFTPServerReachable
- starPPTDBBackupDestinationNotAccessible
- starPPTDBBackupNotEnoughDiskSpace

It was discovered that the following SSC traps had never been documented since they were first added to the MIB in 12.1:

- starSSCLdapInitFailed
- starSSCLdapInitSuccess
- starSSCProfileConTheshCrossed
- starSSCProfileConTheshCleared
- starSSCGeoFailoverStarted
- starSSCGeoFailoverCompleted

The following were incorrectly identified as modified alarms in versions of this document up to and including October 30, 2012, when they are actually conformances that do not need to be documented:

- starSSCObjectGroup
- starSSCNotifGroup
- starPPTNotifMgmtGroup

New Objects

None for this release.

Modified Objects

None for this release

Obsoleted Objects

None for this release.

New Alarms

- starSSCGeoFailoverFailed
- starSSCRoleChangeFailed
- starSSCStopObserverFailed
- starSSCStartObserverFailed
- starSSCScpFSFOFailed
- starSSCCacheCleanupFailed
- starSSCDetDBRoleFailed
- starSSCDataGuardBrokerDown
- starSSCStartListnerFailed
- starSSCMonitoringT10Failed
- starSSCProcessStartFail
- starSSCFTPServerUnreachable
- starSSCFTPServerReachable
- starPPTDBBackupDestinationNotAccessible
- starPPTDBBackupNotEnoughDiskSpace

During an inspection of the SNMP MIB Reference for October 30, 2012, it was discovered that the following SSC traps had never been documented since they were first added to the MIB in 12.1:

- starSSCLdapInitFailed
- starSSCLdapInitSuccess
- starSSCProfileConTheshCrossed
- starSSCProfileConTheshCleared
- starSSCGeoFailoverStarted
- starSSCGeoFailoverCompleted

Modified Alarms

None for this release

Obsoleted Alarms

During a review of the Cisco *ASR 5000 SNMP MIB Reference* for October 2012, it was established that the following SSC traps had been made obsolete in the 12.1 build. In some cases, their trap numbers (in parentheses) have been reused for other traps.

- starSSCPeerStateUp(6)
- starSSCPeerStateDown(7)
- starSSCEmailServerUnreachable(10)
- starSSCEmailServerReachable(11)
- starSSCSmsServerUnreachable(12)
- starSSCSmsServerReachable(13)
- starSSCMaxPendReqAppMgrSysCleared
- starSSCMaxPendReqAppMgrSysCrossed
- starSSCMaxPendReqAppMgrCrossed
- starSSCMaxPendReqAppMgrCleared
- starSSCSprDown
- starSSCSprUp
- starSSCSprCacheDown
- starSSCSprCacheUp

Web Element Manager Path

Select Configuration | SNMP Configuration.

SNMP MIB Objects and Alarms in Release 12.2

This section lists additions and changes to MIB objects and alarms in Release 12.2.

Omissions and Corrections to Past Releases

During a review of the *Cisco ASR 5000 SNMP MIB Reference*, it was discovered that the external management applications had been documented with Object ID strings that were inconsistent with the MIB files present in the software. This affects all releases up to and including 10/31/2012.

In order to correct this, a new hierarchy diagram has been created for each product, and the OID strings have been corrected in the most current user documentation, released 11/30/2012.

This correction is NOT required for the starOS MIB objects; however, a new hierarchy diagram has been added for clarity.

The following table defines the changes for the MIB Objects OID strings. The OID strings continue to be prefaced with “enterprise” to represent 1.3.6.1.4.1:

Application	Previously Documented OID String	Corrected OID String
Content Filtering supports multiple MIBs:		
starCFCommonMIB	enterprise.8164.1.100.1.1.*x*	enterprise.8164.100.1.1.*x*
starCFCDPMIB	enterprise.8164.1.100.2.1.*x*	enterprise.8164.100.2.1.*x*
starCFREMIB	enterprise.8164.1.100.3.1.*x*	enterprise.8164.100.3.1.*x*
starCFCCIMIB	enterprise.8164.1.100.4.1.*x*	enterprise.8164.100.4.1.*x*
starCFEMSMIB		*enterprise.8164.100.5.1.*x*
*enterprise.8164.100.5.1.*x* has been added as a placeholder for possible future development		
starCFMCRDBSMIB	enterprise.8164.1.100.6.1.*x*	enterprise.8164.100.6.1.*x*
IPMS	enterprise.8164.1.102.1.*x*	enterprise.8164.102.1.*x*

Application	Previously Documented OID String	Corrected OID String
MUR	enterprise.8164.1.103.1.*x*	enterprise.8164.103.1.*x*
PPT	enterprise.8164.1.104.1.*x*	enterprise.8164.104.1.*x*
SSC	enterprise.8164.1.201.1.*x*	enterprise.8164.201.1.*x*
WEM	enterprise.8164.1.1000.1.*x*	**enterprise.8164.1.1000.1.*2.x*
**Note that WEM retains the “1” after 8164 and adds “2” to the string		

The following table defines the changes for the MIB Traps OID strings. The OID strings continue to be prefaced with “enterprise” to represent 1.3.6.1.4.1:

Application	Previously Documented OID String	Corrected OID String
Content Filtering supports multiple MIBs:		
starCFCommonMIB	enterprise.8164.1.100.1.1.*x*	enterprise.8164.100.1.1.*x*
starCFCDPMIB	enterprise.8164.1.100.2.1.*x*	enterprise.8164.100.2.1.*x*
starCFREMIB	enterprise.8164.1.100.3.1.*x*	enterprise.8164.100.3.1.*x*
starCFCCIMIB	enterprise.8164.1.100.4.1.*x*	enterprise.8164.100.4.1.*x*
starCFEMSMIB		*enterprise.8164.100.5.1.*x*
*enterprise.8164.100.5.1.*x* has been added as a placeholder for possible future development		
starCFMCRDBSMIB	enterprise.8164.1.100.6.1.*x*	enterprise.8164.100.6.1.*x*
IPMS	enterprise.8164.1.102.1.*x*	enterprise.8164.102.1.*x*
MUR	enterprise.8164.1.103.1.*x*	enterprise.8164.103.1.*x*
PPT	enterprise.9.1.787.1.*x*	enterprise.9.9.787.0.*x*
SSC	enterprise.8164.1.201.1.*x*	enterprise.8164.201.1.*x*
WEM	enterprise.8164.1.1000.1.*x*	**enterprise.8164.1.1000.1.*2.x*
**Note that WEM retains the “1” after 8164 and adds “2” to the string		

The following table defines the changes for the MIB Conformances OID strings. The OID strings continue to be prefaced with “enterprise” to represent 1.3.6.1.4.1:

The most common finding was that MIBGroups and MIBCompliances OID strings were reversed in some cases. Although not all applications were affected, the following is the correct OID string for *all* applications, corrected as per the MIB file, as reflected in the most current user documentation of 11/30/2012:

Application	OID String
starCFCommonMIB	Possible future development
starCFCDPMIB	Possible future development
starCFREMIB	enterprise.8164.100.3.3.starCFREMIBGroups(1).x enterprise.8164.100.3.3.starCFREMIBCompliances(2).x
starCFCCIMIB	enterprise.8164.100.4.3.starCFCCIMIBGroups(1).x enterprise.8164.100.4.3.starCFCCIMIBCompliances(2).x
starCFEMSMIB	Possible future development
starCFMCRDBSMIB	enterprise.8164.100.6.3.starCFMCRDBSMIBGroups(1).x enterprise.8164.100.6.3.starCFMCRDBSMIBCompliances(2).x
starEMSMIB (WEM)	enterprise.8164.1.1000.3.starEmsMIBCompliances(1).x enterprise.8164.1.1000.3.starEmsMIBGroups(2).x
starIPMSMIB	enterprise.8164.102.3.starIPMSMIBCompliances(1).x enterprise.8164.102.3.starIPMSMIBGroups(2).x
starMURMIB	enterprise.8164.103.3.starMURMIBGroups(1).x enterprise.8164.103.3.starMURMIBCompliances(2).x
starPPTMIB	enterprise.8164.104.3.starPPTMIBGroups(1).x enterprise.8164.104.3.starPPTMIBCompliances(2).x
starSSCMIB	enterprise.8164.201.3.starSSCMIBGroups(1).x enterprise.8164.201.3.starSSCMIBCompliances(2).x
For the WEM application, see starEMSMIB	

New Objects

- StarCLIDatabaseUsername
- starPCCNtfyIntfPeerName
- starSessGTPPGroupName
- starMMES1PathTable
- starMMES1PathEntry
- starMMES1PathSvcID
- starMMES1PathENBID
- starMMES1PathVpnName
- starMMES1PathServName
- starMMES1PathSelfAddr
- starMMES1PathSelfPort
- starMMES1PathPeerAddr
- starMMES1PathPeerPort
- starLAGPartner
- starECSTotalDNSLearntIPThresholdInstance
- starECSTotalDNSLearntIPThresholdconfigured
- starECSTotalDNSLearntIPThresholdmeasured
- starPeerAddressIpv6

Modified Objects

- StarGGSNSerEntry
- starPCFSvcID

The description has been modified to read:

The service identification is made up from first 8 chars of the context name and the first 8 chars of the service name separated by (:), with the length of this structure at the beginning.

- starentCardType

The following hardware Enumerations apply as of April 30, 2012:

- fanctrl6(28) -- Fan control revision 6
- vioc(29) -- Virtual I/O Card
- gpdsp(30) -- GP-DSP Daughter Card
- xme(31), --XME Daughter Card
- vop(32) -- VOP Daughter Card
- edc(33) -- EDC Card
- mio(34) -- Management & I/O Card
- mio10g10p(35) -- Management & 10x10Gb I/O Card
- mio10g20p(36) -- Management & 20x10Gb I/O Card
- mio40g2p(37) -- Management & 2x40Gb I/O Card

- mio40g4p(38) -- Management & 4x40Gb I/O Card
- mio40g12p(39) -- Management & 12x40Gb I/O Card
- miodc(40) -- MIO Daughter Card
- fsc(41) -- Fabric Card
- dpc(42) -- Data Processing Card
- mdpc(43) -- M Data Processing Card
- dpcdc(44) -- DPC Daughter Card
- ssc(45) -- System Status Card
- StarentCardType

The following hardware Enumerations apply as of March 30, 2012:

- lcchan3p2(26) -- Channelized Line Card 2 Port
- lcchan3p4(27) -- Channelized Line Card 4 Port
- vioc(28) -- Virtual I/O Card
- gpdsp(39) -- GP-DSP Daughter Card
- xme(30), --XME Daughter Card
- vop(31) -- VOP Daughter Card
- edc(32)

The following objects have been modified with the addition of new optional OID strings and a new CLI. These are described in the “SNMP Issues” section of the *Cisco ANA Management Application Integration MIBs* chapter in the *Cisco ASR 5000 Series SNMP MIB Reference.*

- sysDesc
- sysObjectId

Obsoleted Objects

- None for this release

Deleted Objects

None for this release.

New Alarms

- starThreshCardTemperatureNearPowerOffLimit
- starThreshClearCardTemperaturePowerOffLimit
- starAAAArchiveStarted
- starThreshAAAAcctArchiveQueue-1
- starThreshClearAAAAcctArchiveQueue-1
- starThreshAAAAcctArchiveQueue-2
- starThreshClearAAAAcctArchiveQueue-2
- starThreshAAAAcctArchiveQueue-3
- starThreshClearAAAAcctArchiveQueue-3

- starIPSecNodePeerDown
- starIPSecNodePeerUp
- starCdrPurged
- starLocalUserAdded
- starLocalUserRemoved
- starLocalUserPrivilegeChanged
- starOsShellAccessed
- starTestModeEntered
- starLicenseFeaturesModified
- starHiddenAccessEnabled
- starHiddenAccessDisabled
- starLawfulInterceptChanged
- starMMES1PathFail
- starMMES1PathSetup
- starAAAArchiveStarted
- starIPsecNodeIpv6PeerDown
- starIPsecNodeIpv6PeerUPstarAAAArchiveStarted
- starLAGGroupDown
- starLAGGroupUp
- starECSTotalDNSLearntIPv4Threshold
- starECSTotalDNSLearntIPv4ThresholdClear
- starECSTotalDNSLearntIPv6Threshold
- starECSTotalDNSLearntIPv6ThresholdClear
- starECSTotalDNSLearntIPv6Threshold
- starECSTotalDNSLearntIPv6ThresholdClear

Modified Alarms

The following alarms have changed trap numbers as follows:

- starECSTotalDNSLearntIPv4Threshold is now trap 1192
- starECSTotalDNSLearntIPv4ThresholdClear is now trap 1193

The following alarms have changed trap numbers as follows:

- starAAAArchiveStarted from 1191 to 1197
- starECSTotalDNSLearntIPv4Threshold 1192 to 1198
- starECSTotalDNSLearntIPv4ThresholdClear 1193 to 1199
- starECSTotalDNSLearntIPv6Threshold1194 to 1200
- starECSTotalDNSLearntIPv6ThresholdClear 1195 to 1201

Obsoleted Alarms

- starPowerFilterUnitFailed

- starThreshPortSpecRxUtil
- starThreshClearPortSpecRxUtil
- starThreshPortSpecTxUtil
- starThreshClearPortSpecTxUtil

Web Element Manager Path

Select Configuration | SNMP Configuration.

Cisco MIB Objects and Alarms

The following MIBs are used to make an ASR 5x00 chassis available to customers using the Cisco network management applications. The following are supported in releases 12.0 and 12.2.

- IF-MIB
- ENTITY-MIB

The following are supported in release 12.2 only.

- CISCO-ENTITY-FRU-CONTROL-MIB
- CISCO-ENTITY-STATE-MIB

Please refer to the Appendix in the *Cisco ASR 5000 Series SNMP MIB Reference* for more information.

Web Element Manager Fault Management

This section describes the Fault Management changes made in WEB Element Manager Releases 12.0 and 12.2.

Web Element Manager Release 12.0

The following enhancements were made to WEM Release 12.0.

Addition to fm.cfg File for Setting Alarm Info Location Field

A new section has been introduced to the *fm.cfg* file for setting the *location* field in the alarm information, as follows:

- Display card and port numbers only for card (hardware) related alarms. Setting this configuration will show only the card and port number instead of the complete varbind object list. WEM will show this information based on the value of the starSlotNum and ifindex objects. A WEM server restart is required.

  The format is <*card-number/port-number*>.

  Possible values are:

  - ENABLE: Shows only card/port value in location information for card alarms. This is the default value.
  - DISABLE: Show the values in default format with complete object information.
  - UseCardPortNumber = ENABLE.
- All the WEM specific alarms have a varbind object starEmsNotifRaisedTime which carries the time when WEM generated the trap. This varbind object can be skipped in the *location* field. A WEM server restart is required.

  Possible values are:

  - ENABLE: Skips the starEmsNotifRaisedTime varbind object. This is the default value.
  - DISABLE: Shows the starEmsNotifRaisedTime varbind object.
  - SkipWEMEventTimeObject = ENABLE.
- For alarms generated for SNMPv2 traps there are two standard SNMPv2 varbind objects (snmpTrapOid and sysUpTime). These varbind objects can be skipped in the *location* field.

  Also, note that for card/port related alarms, the value of the UseCardPortNumber parameter will override the configuration.

  A WEM server restart is required.

  - ENABLE: Skips the SNMPv2 trap objects snmpTrapOid and sysUpTime. This is the default value.
  - DISABLE: Shows the SNMPv2 standard objects.
  - SkipSNMPv2StdObjects = ENABLE

Web Element Manager Path

- On the WEM server: <*ems_dir*>/server/etc/fm.cfg

Web Element Manager Release 12.2

The following Fault Management changes were made in Web Element Manager Release 12.2.

Adding, Deleting or Modifying a WEM User will Create Alarm

Previous Behavior: No alarm was generated whenever a WEM user was added, deleted or modified.

Modified Behavior: As part of an ongoing effort to increase WEM security, an alarm will be generated whenever a WEM user is added, deleted or modified.

Alarm View Sorting by Severity

Previous Behavior: Any Alarm View screens were sorted alphabetically.

Modified Behavior: This has been changed so sort them by status in descending order from Critical to Clear.

Name Resolution in Current Alarm Screen

Previous Behavior: In the Current Alarm screen, the Location field showed the Hostname for the chassis being managed, but showed the IP address for any other configured Network Element (NE).

Modified Behavior: The Location field now shows the Hostname for the managed chassis, WEM and any other configured NE. An example of this might be if MUR is configured as an NE in order to display MUR alarms forwarded to WEM.

WEM Online Help path to this screen is Alarm Menu\Current Alarm View\Dialog Boxes\Current Alarm View. The help page will be updated shortly.

New Northbound Interface IRP Table Traps

WEM supports the Northbound Interface as defined in the 3GPP standards for Telecom Management. 3GPP defines a standard interface (Interface-N) between the EMS and the NMS. It also defines Integration Reference Points (IRPs) through which various aspects of system management (FCAPS) are performed by the NMS.

Previous Behavior: Support for *unacknowledge_Alarms* and *acknowledge_Alarms* was not provided.

Modified Behavior: Support for *unacknowledge_Alarms* and *acknowledge_Alarms* has been added. These appear in the Alarm Operations category in the IRP table in the *Overview* chapter in the *Cisco Web Element Manager Installation and Administration Guide*.

Port 0 is Displayed in Current Alarm View Description Field

Previous Behavior: “Port 0” could be displayed in the Current Alarm view description field although a port “Port 0” could not exist in a configuration.

Modified Behavior: “Port 0” can no longer be displayed as part of a description.

Time Detail in Alarm View Location Field Configurable

Previous Behavior: The Location field in the WEM Alarm View contains time information by default.

Modified Behavior: A new configurable has been added to the *fm.cfg* file to offer the option to display time information or not.

skipStarbindLocation has the default value of “Disable” so all varbind objects are displayed. If it is set to “Enable,” only the trap source name is displayed.

WEM Integration with Mobility Unified Reporting (MUR)

Previous Behavior: MUR alarms could not be forwarded upstream to be displayed in WEM.

Modified Behavior: MUR can now be configured as a Network Element (NE) through the WEM Configuration menu. This means that MUR can be configured to forward alarms to WEM to be managed through options in the Alarm Management menu.

Currently, WEM integration with MUR is limited to alarms, and some MIBs are not yet integrated. If the MIB is not integrated, the alarm ID would be displayed instead of the alarm name. Users should be aware that although WEM will synchronize with MUR, there may be a time delay before the alarms are updated.

A number of WEM Online Help pages have been updated; see the following table for the path to each page.

You can also refer to the *Cisco Mobility Uniform Reporting Administration Guide*, and the MUR Online Help for more information.

Menu Path	Page Title
Configuration Menu\NE List\Procedures	Procedure: Adding a Network Element (System Device) Modifying a Network Element (System Device)
Configuration Menu\NE List\Dialog Boxes	NE List Dialog Box NE List Dialog Box - SSC/MUR Tab Add NE Dialog Box Add NE Dialog Box - SSC/MUR Tab Modify NE Dialog Box Modify NE Dialog Box - SSC/MUR Tab
Alarm Management Menu\Current Alarm View\Dialog Boxes	Current Alarm View Set Alarm Filter Configuration Dialog Box Set Alarm Forwarding Filter Dialog Box

Menu Path	Page Title
Alarm Management Menu\Pending Alarm Menu\Dialog Boxes	Pending Alarm View
Alarm management Menu\Historical Alarm View\Dialog Boxes	Set Historical Alarm Filter - Alarm Database Dialog Box
Monitor Test Menu\Monitoring Operations Submenu\EMS Server Process Monitoring\Dialog Boxes	WEM Process Monitoring Dialog Box

CHAPTER 3
CONFIGURATION MANAGEMENT

This chapter identifies new, modified, and obsoleted configuration commands in Releases 12.0, 12.1, and 12.2.

Topics covered in this chapter are:

New Configuration Commands

This section identifies configuration commands that are new in Release 12.x.

Common Commands - New in Release 12.0

This section provides information on new commands that are common to products in Release 12.0.

aaa secondary-group

This command enables to configure secondary AAA group for the APN. This supports the RADIUS Fire-and-Forget feature in conjunction with GGSN for secondary accounting (with different RADIUS accounting group configuration) to the RADIUS servers without expecting acknowledgement from the server, in addition to standard RADIUS accounting. This secondary accounting will be an exact copy of all the standard RADIUS accounting message (RADIUS Start / Interim / Stop) sent to the standard AAA RADIUS server.

CLI (APN Configuration Mode)

aaa secondary-group *aaa_group_name*

{ default | no } aaa secondary-group

aaa tacacs+

Enables TACACS+ AAA services that have been configured on the ASR 5000.

CLI (Global Configuration Mode)

aaa tacacs+

aaa secondary-group

This command enables to configure secondary AAA group for the subscriber template. This supports the No-ACK RADIUS Targets feature in conjunction with PDSN and HA for secondary accounting (with different RADIUS accounting group configuration) to the RADIUS servers without expecting the acknowledgement from the server, in addition to standard RADIUS accounting. This secondary accounting will be an exact copy of all the standard RADIUS accounting message (RADIUS Start / Interim / Stop) sent to the standard AAA RADIUS server.

CLI (Subscriber Configuration Mode)

aaa secondary-group *aaa_group_name*

{ default | no } aaa secondary-group

accounting

Enables or disables the recording of the start and stop time of each command issued during a TACACS+ authenticated session.

CLI (TACACS+ Configuration Mode)

[no] accounting { start-stop | command }

app-level-retransmission

This command enables application-level retransmissions with “T” bit set.

CLI (Credit Control Configuration Mode)

app-level-retransmission { set-retransmission-bit | unset-retransmission-bit }

default app-level-retransmission

arp-priority-level

This command enables to map ARP priority-level value received from PCRF to inter-user-priority value and be sent in A11 session update.

CLI (Policy Control Configuration Mode)

arp-priority-level map-to inter-user-priority

{ default | no } arp-priority-level map-to

authorization

Enables or disables the authorization of TACAS+ users on a command-by-command, command + argument, or command prompt basis.

CLI (TACACS+ Configuration Mode)

[no] authorization { command | prompt | arguments }

cc-profile

This command enables to configure value of the Offline AVP sent by GGSN to the PCRF over Gx interface based on the Charging Characteristics (CC) profile received from the SGSN.

CLI (Policy Control Configuration Mode)

cc-profile *cc_profile_number* **[to** *cc_profile_number_range_end* **] map-to offline-avp { 0 | 1 }**

{ default | no } cc-profile

credit-control-group

This command enables to configure Credit Control Group in subscriber template.

CLI (Subscriber Configuration Mode)

credit-control-group *cc_group_name*

no credit-control-group

diameter fui-redirected-flow

This command enables to control the behavior of marking redirected HTTP flow as free-of-charge when the Final-Unit-Indication (FUI) Diameter AVP comes without Filter IDs.

CLI (Credit Control Configuration Mode)

[no] diameter fui-redirected-flow allow

diameter ignore-service-id

This command enables to accept/ignore service ID in Service-Identifier AVP defined in the Diameter dictionaries for Gy interface implementation.

CLI (Credit Control Configuration Mode)

[default | no] diameter ignore-service-id

diameter service-context-id

This command configures the value to be sent in the Service-Context-Id AVP, which identifies the context in which DCCA is used.

CLI (Credit Control Configuration Mode)

diameter service-context-id *service_context_id*

default diameter service-context-id

diameter update-dictionary-avps

This command enables dictionary control of the AVPs that need to be added based on the version of the specification to which the OCS is compliant with. This command is applicable to all products that use the dcca-custom8 dictionary for Gy interface implementation.

CLI (Credit Control Configuration Mode)

diameter update-dictionary-avps { 3gpp-rel8 | 3gpp-rel9 }

{ default | no } diameter update-dictionary-avps

diameter update-dictionary-avps

This command enables dictionary control of the AVPs that need to be added based on the version of the specification to which the PCEF is compliant with. This command is applicable only to Diameter dictionaries that support standard based volume reporting over Gx feature.

CLI (Policy Control Configuration Mode)

diameter update-dictionary-avps { 3gpp-r8 | 3gpp-r9 }

{ default | no } diameter update-dictionary-avps

destination-host-avp

This command controls encoding of the Destination-Host AVP in initial/retried requests.

CLI (Diameter Endpoint Configuration Mode)

destination-host-avp { session-binding | always | initial-request | retried-request }

default destination-host-avp

dynamic-peer-failure-retry-count

This command configures the number of times the system attempts to connect to a dynamically discovered Diameter peer.

CLI (Diameter Endpoint Configuration Mode)

dynamic-peer-failure-retry-count *value*

default dynamic-peer-failure-retry-count

dynamic-route

This command configures the expiration time for dynamic routes created after a Diameter destination host is reached.

CLI (Diameter Endpoint Configuration Mode)

dynamic-route expiry-timeout *value*

default dynamic-route expiry-timeout

egcdr cdr-encoding

This command configures the eG-CDR encoding type.

CLI (ACS Rulebase Configuration Mode)

egcdr cdr-encoding { ascii [delimiter { colon | comma | pipe }] | asn.1 }

default egcdr cdr-encoding

gtpp egcdr rulebase-max-length

This command is used to configure the maximum length of charging rulebase name in LOSDVs of eG-CDRs/PGW-CDRs to be between 1 and 63 characters. If configured to 0 (zero) the rulebase name is not trimmed. This CLI command is now available in 12.0 and later releases.

CLI (Context Configuration Mode & GTPP Group Configuration Mode)

gtpp egcdr rulebase-max-length *rulebase_name_max_length*

no gtpp egcdr rulebase-max-length

link-aggregation port switch to

When a link aggregation group (LAG) contains two sets of ports, each connecting to a different Ethernet switch, this command allows you to change the status of the active distributing ports.

CLI (Exec Mode)

link-aggregation port switch to *slot_num/port_num*

load-balancing-algorithm

This command configures the behavior for load balancing Diameter peers in the event of a failure of an active server.

CLI (Diameter Endpoint Configuration Mode)

load-balancing-algorithm { highest-weight | lowest-weight-borrowing min-active-servers *number* **}**

default load-balancing-algorithm

lsp ping

This command checks the Multi Protocol Label Switching (MPLS) LSP connectivity for the specified Forwarding Equivalence Class (FEC). It must be followed by an IPv4 prefix.

CLI (Exec Mode)

lsp-ping *ip_prefix_FEC* **[count** *ping-packets* **] [| verbose] [| grep** *grep_options* **]**

lsp-traceroute

This command discovers MPLS LSP routes that packets actually take when traveling to their destinations. It must be followed by an IPv4 prefix.

CLI (Exec Mode)

lsp-traceroute *ip_prefix_FEC* **[maxttl** *time_to_live* **] [| verbose] [| grep** *grep_options* **]**

on-authen-fail

Defines system behavior when an administrative login fails due to a TACACS+ authentication failure.

CLI (TACACS+ Configuration Mode)

on-authen-fail { continue | stop } [tty console]

on-network-error

Defines system behavior when a TACACS+ login fails due to a network error.

CLI (TACACS+ Configuration Mode)

on-network-error { continue | stop } [tty console]

on-unknown-user

Configures system behavior when a TACACS+ server cannot authenticate a given user name.

CLI (TACACS+ Configuration Mode)

on-unknown-user { continue | stop } [tty console]

policy-control bind-default-bearer

For PCEF bearer binding in 3G and when BCM mode is UE_ONLY, this command does not bind rules with QCI of default bearer to the default bearer and does not ignore other rules.

When BCM of UE_ONLY is received from PCRF, P-GW/GnGp P-GW will not terminate the call.

CLI (ACS Configuration Mode)

[default | no] policy-control bind-default-bearer

policy-control update-default-bearer

For PCEF bearer binding in LTE, this command enables updates, like TFT and bit rates, towards MS in downlink direction on default bearer. This allows application of pre-defined ECS based rules on default bearer.

CLI (ACS Configuration Mode)

[default | no] policy-control update-default-bearer

post-processing policy

This command configures the post-processing policy to be applied on Limit-Reached packets. This allows to enable post-processing priority based rules for content in blacklisted state.

The **post-processing policy always** CLI command will enable post-processing on Limit-Reached packets. If there are post-processed priority based rules, it will check for any redirection rules, else will discard the packets by default. No other post-processing actions like forward, next-hop, xheader-insertion, etc. will be applied on these limit-reached packets. If no post-processing priority rules are present, the packets will be dropped by default.

The **post-processing policy not-for-dynamic-discard** will directly discard the limit-reached context and will not apply post-processing priority based rules. This is the default setting.

Also, refer to the configuration changes required in the *New Feature Summary* chapter.

CLI (ACS Rulebase Configuration Mode)

post-processing policy { always | not-for-dynamic-discard }

default post-processing policy

pptp any-match

This command defines rule expressions to match all PPTP packets. This is used in conjunction with ADC, Stateful Firewall, and NAT in-line services.

CLI (ACS Ruledef Configuration Mode)

[no] pptp any-match *operator condition*

pptp ctrl-msg-type

This command defines rule expressions to analyze and charge user traffic based on control message type for PPTP packets. This is used in conjunction with ADC, Firewall, and NAT inline services.

CLI (ACS Ruledef Configuration Mode)

[no] pptp ctrl-msg-type = { call-clear-request | call-disconnect-notify | echo-reply | echo-request | incoming-call-connected | incoming-call-reply | incoming-call-request | outgoing-call-reply | outgoing-call-request | set-link-info | start-control-connection-reply | start-control-connection-request | stop-control-connection-reply | stop-control-connection-request | wan-error-notify

pptp gre

This command defines rule expressions based on GRE to match all PPTP packets. This is used in conjunction with ADC, Firewall, and NAT in-line services.

CLI (ACS Ruledef Configuration Mode)

[no] pptp gre any-match = *condition*

radius accounting fire-and-forget

This feature enables to configure the Fire-and-Forget feature. The accounting request sent to a RADIUS accounting server configured under the AAA group with this CLI command configured in it will not expect a response from the server.

CLI (AAA Group Configuration Mode)

[default | no] radius accounting fire-and-forget

require ecs credit-control subscriber-mode

This command configures DCCA/Gy to work in per subscriber-PDN level Gy mode, wherein one Diameter session is created per subscriber PDN rather than per bearer, and only one DCCA/Gy session is created for multi-bearer PDNs. This command is applicable to all products using the Gy interface.

CLI (Global Configuration Mode)

[no] require ecs credit-control subscriber-mode

server

Configures TACACS+ AAA service-related parameters for use in authenticating ASR 5000 administrative users via a TACACS+ server.

CLI (TACACS+ Configuration Mode)

[no] server priority *priority_number* **ip-address** *ip_address* **[service { authentication | authorization | accounting }] [port** *port_number* **] [{ encrypted password** *shared_secret* **| password** *text_password* **}] [timeout** *seconds* **] [retries** *num_retries* **] [nas-source-address** *ip_address* **]**

server-mode

This command configures the Diameter endpoint to establish the system as the server side endpoint of the connection.

CLI (Diameter Endpoint Configuration Mode)

server-mode [demux-mode]

servers-unreachable

This command configures whether to continue/terminate calls when Diameter server(s)/OCS become unreachable.

CLI (Credit Control Configuration Mode)

servers-unreachable { initial-request { continue | terminate [after-timer-expiry *timeout_period* **] } | update-request { continue | terminate [after-quota-expiry | after-timer-expiry** *timeout_period* **] } }**

no servers-unreachable { initial-request | update-request }

Common Commands - New in Release 12.2

This section provides information on new commands that are common to products in Release 12.2.

associate

The **associate** command allows the Diameter endpoint configuration to be associated with SCTP parameters configured in a template. In this release, this command replaces the **diameter sctp** command in the Context Configuration mode.

For more information on the deprecated command, please see the *diameter sctp* command in the *Common Commands - Obsoleted in Release 12.2* section.

CLI (Diameter Endpoint Configuration Mode)

associate sctp-parameters-template *template_name*

no associate sctp-parameters-template

chassis

The Exec mode **chassis key value** *key_string* command identifies the chassis which can encrypt and decrypt encrypted passwords in the configuration file. If two or more chassis are configured with the same chassis key value, the encrypted passwords can be decrypted by any of the chassis sharing the same chassis key value. As a corollary to this, a given chassis key value will not be able to decrypt passwords that were encrypted with a different chassis key value.

The *key_string* is an alphanumeric string of 1 through 16 characters. The chassis key is stored as a one-way encrypted value, much like a password. For this reason, the chassis key value is never displayed in plain-text form.

The Exec mode **chassis keycheck** *key_string* command generates a one-way encrypted key value based on the entered key_string. The generated encrypted key value is compared against the encrypted key value of the previously entered chassis key value. If the encrypted values match, the command succeeds and keycheck passes. If the comparison fails, a message is displayed indicating that the key check has failed. If the default chassis key (no chassis key) is currently being used, this key check will always fail since there will be no chassis key value to compare against.

Use the chassis keycheck command to verify whether multiple chassis share the same chassis key value.

CLI (Exec Mode)

chassis {key value <key_string> **| keycheck** <key_string>

Application Detection and Control - New in Release 12.0

This section provides information on new ADC commands available in Release 12.0.

None for this release.

Application Detection and Control - New in Release 12.2

This section provides information on new ADC commands available in Release 12.2.

None for this release.

ASN GW Commands - New in Release 12.0

This section provides information on new ASN GW commands available in Release 12.0.

asn-policy ms-requested-classifiers

This command allows an operator to allow or decline the dynamic addition of classifiers during MS-initiated service flow creation/modification.

CLI (Subscriber Configuration Mode)

[no] asn-policy ms-requested-classifiers { allow | disallow }

asn-policy notification-handoff

This command allows an operator to enable/disable the reporting of the BSID in the Accounting Interim Update during the handoff and location update.

CLI (Subscriber Configuration Mode)

[no] asn-policy notification-handoff { allow | disallow }

asn-policy hotlining wimax

This command allows an operator to enable or disable WiMAX hotlining capability in the ASNGW and WiMAX HA. The command applies to both profile id-based and rule-based hotlining.

CLI (Subscriber Configuration Mode)

[no] asn-policy hotlining-wimax

asngw-service priority vlan

This command allows an operator to enable or disable 802.1P priority marking for WiMAX control traffic over an R6/R4 interface.

CLI (Service Configuration Mode)

asngw-service *asngw_servicename* **priority vlan** *priority*

The default is to disallow.

schedule-type

This command allows an operator to configure the 802.1 priority based on the schedule type for WiMAX data traffic.

CLI (ASN QoS Descriptor Configuration Mode)

[no] schedule-type [be | ertvr | nrtvr | rtvr | ugs] priority *priority*

If the policy is set to allow, only the priority value is used for WiMAX data traffic.

Content Filtering Commands - New in Release 12.0

This section provides information on new CF commands available in Release 12.0.

None for this release.

ECS Commands - New in Release 12.0

This section provides information on new ECS commands available in Release 12.0.

egcdr cdr-encoding

This command configures the eG-CDR encoding type. When configuring the eG-CDR encoding type as ASCII, the delimiter character can be specified as either ":" (colon), "," (comma), or "|" (pipe). The default delimiter character is "|" (pipe).

CLI (ACS Rulebase Configuration Mode)

egcdr cdr-encoding { ascii [delimiter { colon | comma | pipe }] | asn.1 }

default egcdr cdr-encoding

http domain

This command enables to define rule expressions to match domain portion of the URI in HTTP packets.

CLI (ACS Ruledef Configuration Mode)

[no] http domain [case-sensitive] *operator domain*

tcp proxy-prev-state

This command defines rule expressions to match TCP previous state on the ingress side of the TCP proxy.

CLI (ACS Ruledef Configuration Mode)

[no] tcp proxy-prev-state *operator previous_state*

tcp proxy-state

This command defines rule expressions to match TCP state on the ingress side of the TCP proxy.

CLI (ACS Ruledef Configuration Mode)

[no] tcp proxy-state *operator previous_state*

tftp any-match

This command defines rule expressions to match all TFTP packets.

CLI (ACS Ruledef Configuration Mode)

[no] tftp any-match *operator condition*

tftp data-any-match

This command defines rule expressions to match all TFTP data packets.

CLI (ACS Ruledef Configuration Mode)

[no] tftp data-any-match *operator condition*

wsp domain

This command enables to define rule expressions to match domain portion of the URI in WSP packets.

CLI (ACS Ruledef Configuration Mode)

[no] wsp domain [case-sensitive] *operator domain*

www domain

This command enables to define rule expressions to match domain portion of the URI for WSP/HTTP packets.

CLI (ACS Ruledef Configuration Mode)

[no] www domain [case-sensitive] *operator domain*

ECS Commands - New in Release 12.2

This section provides information on new ECS commands available in Release 12.2.

edr sn-charge-volume

This command enables to exclude/include packets/bytes dropped/retransmitted by ECS in the total charge volume — sn-charge-volume EDR attribute.

CLI (ACS Rulebase Configuration Mode)

[default | no] edr sn-charge-volume { count-dropped-units | count-retransmitted-units }

fair-usage tcp-proxy

This command configures the maximum number of flows for which TCP Proxy can be used per subscriber, and what portion of ECS memory should be reserved for TCP Proxy flows.

CLI (ACS Configuration Mode)

fair-usage tcp-proxy { max-flows-per-subscriber *max_flows* **| memory-share** *memory_share* **}**

ip dns-learnt-entries

This command configures how long to keep the snooped addresses that were extracted from DNS responses.

CLI (ACS Configuration Mode)

ip dns-learnt-entries timeout *timeout_period*

{ default | no } ip dns-learnt-entries timeout

ip server-domain-name

This command defines rule expressions to match host names (domain names).

CLI (ACS Ruledef Configuration Mode)

[no] ip server-domain-name *operator domain_name*

policy-control bearer-bw-limit

This command allows you to enable/disable per-bearer MBR policing—bandwidth limiting. Note that there are only two variants of this command, the default and no variants.

{ default | no } policy-control bearer-bw-limit

policy-control dynamic-rule-limit

This command allows you to enable/disable per-dynamic-rule MBR policing—bandwidth limiting. Note that there are only two variants of this command, the default and no variants.

{ default | no } policy-control dynamic-rule-limit

tethering-database

This command enables the Tethering Detection feature, and loads the databases from the specified files into the service.

CLI (ACS Configuration Mode)

tethering-database [os-signature *os_signature_db_file_name* **| tac** *tac_db_file_name* **| ua-signature** *ua_signature_db_file_name* **] +**

{ default | no } tethering-database

tethering-detection

This command defines rule expressions to match tethered/non-tethered flows.

CLI (ACS Ruledef Configuration Mode)

tethering-detection { flow-not-tethered | flow-tethered }

no tethering-detection

tethering-detection

This command enables/disables the Tethering Detection feature for a rulebase, and configures the database to use.

CLI (ACS Rulebase Configuration Mode)

```
tethering-detection [ os-db-only | ua-db-only ]
{ default | no } tethering-detection
```

upgrade tethering-detection

This command upgrades the Tethering Detection feature's database(s).

CLI (Exec Mode)

```
upgrade tethering-detection database { all | os-signature | tac |
ua-signature } [ -noconfirm ]
```

Firewall Commands - New in Release 12.0

This section provides information on new Stateful Firewall commands available in Release 12.0.

icmpv6 any-match

This command configures an access ruledef to match any ICMPv6 traffic for the user.

CLI (Access Ruledef Configuration Mode)

```
[ no ] icmpv6 any-match operator condition
```

icmpv6 code

This command configures an access ruledef to analyze user traffic based on ICMPv6 code.

CLI (Access Ruledef Configuration Mode)

```
[ no ] icmpv6 code operator code
```

icmpv6 type

This command configures an access ruledef to analyze user traffic based on ICMPv6 type.

CLI (Access Ruledef Configuration Mode)

```
[ no ] icmpv6 type operator type
```

ip version

This command defines rule expressions to match version number in IP header.

CLI (Access Ruledef Configuration Mode)

```
[ no ] ip version = { ipv4 | ipv6 }
```

Firewall Commands - New in Release 12.2

This section provides information on new Stateful Firewall commands available in Release 12.2.

None for this release.

GGSN Commands - New in Release 12.0

This section provides information on new GGSN commands available in Release 12.0.

ikev1 disable-initial-contact

From the Context Configuration Mode, this command disables the sending of an INITIAL-CONTACT message in the IKEv1 protocol after the node creates a new Phase 1 SA, caused either by Dead Peer Detection or by a rekey.

CLI (Context Configuration Mode)

```
[ no ] ikev1 disable-initial-contact
```

dhcp chaddr-validate

This CLI has been introduced to skip the client hardware address (chaddr) validation performed on DHCPACK Message. This is required because some of the corporate DHCP servers in the field are not compliant with RFC 2131 and are not sending exact chaddr in DHCPACK message as it has received in DHCPREQUEST message. Configuring **"no dhcp chaddr-validate"** CLI will ensure that the chaddr field in DHCPACK is not validated and call is successfully established. Existing default behavior is to perform chaddr validation and if mismatch is detected call gets rejected.

CLI (DHCP Service Configuration mode)

```
[ default | no ] dhcp chaddr-validate
```

GGSN Commands - New in Release 12.2

This section provides information on new GGSN commands available in Release 12.2.

sequence-number

This command enables addition of the sequence number to every GTP-U packet. Default is disabled.

CLI (GTP-U Service Configuration Mode)

```
[ no ] sequence-number
```

HA Commands - New in Release 12.0

This section provides information on new HA commands available in Release 12.0.

None for this release.

HNB-GW Commands - New in Release 12.1

This section provides information on new commands for HNB-GW available in Release 12.1.

map lac

This command configures the mapping of Location Area Code (LAC) received from UE to MSC point code. This is an important configuration for CS network resource sharing without Iu-Flex interface configuration.

Support for multiple MSC selection in a CS core network is provided with this command.

CLI (HNB-CS Configuration Mode)

map lac range *lac_start* **to** *lac_end* **point-code** *msc_point_code*

no map lac range *lac_start* **to** *lac_end*

ecmp-lag hash

This command is added to the Global Configuration Mode to configure the system to select source Boxer Internal Address (SBIA) as the input to the hashing function for ECMP-LAG distribution.

This command allows the operator to change the way hashing works in deciding which link to use for ECMP and Link Aggregation. In the default hashing algorithm the IP Source Address, IP Destination Address, IP Protocol and Source BIA are used in the hashing function. When “use-sbia-only” option is selected, only the Source BIA is used in the hashing function.

CLI (Global Configuration Mode)

[no] ecmp-lag hash use-sbia-only

CAUTION

While using ECMP-LAG on a HNB-GW, this configuration is **mandatory** for standalone HNB-GW deployment and highly recommended in other deployment scenarios where HNB-GW is used in combination with other services.

HSGW Commands - New in Release 12.0

This section provides information on new HSGW commands available in Release 12.0.

a11-signalling-packets

This command enables the DSCP marking feature for IP headers carrying outgoing A11-signalling A11 packets (such as RRP, RU, SU).

CLI (HSGW Service Configuration Mode)

a11-signalling-packets ip-header-dscp *value*

[default | no] a11-signalling-packets ip-header-dscp

mobility-option-type-value

This command changes the mobility option type value used in mobility messages.

CLI (MAG Service Configuration Mode)

mobility-option-type-value { custom1 | standard }

default mobility-option-type-value

rsvp

This command configures resource reservation protocol (RSVP) parameters for this HSGW service in support of the network initiated QoS feature.

CLI (HSGW Service Configuration Mode)

rsvp { max-retransmissions *count* **| retransmission-timeout** *seconds* **}**

[default | no] rsvp { max-retransmissions | retransmission-timeout }

signalling-packets

This command enables the DSCP marking feature for IP headers carrying outgoing signalling packets.

CLI (MAG Service Configuration Mode)

signalling-packets ip-header-dscp *value*

[default | no] signalling-packets ip-header-dscp

HSGW Commands - New in Release 12.2

This section provides information on new HSGW commands available in Release 12.2.

max-pdn-connections

This command is used to specify the maximum number of eHRPD PDNs supported per session.

CLI (Subscriber Configuration Mode)

max-pdn-connections *eHRPD_PDNs*

default max-pdn-connections

network-initiated-qos

This command is used to enable or disable support for network initiated QoS functionality. Network initiated QoS is enabled by default.

CLI (HSGW Service Configuration Mode)

[default | no] network-initiated-qos

sequence-number

This command enables addition of the sequence number to every GTP-U packet. Default is disabled.

CLI (GTP-U Service Configuration Mode)

`[ no ] sequence-number`

IPCF Commands - New in Release 12.1

This section provides information on new IPCF commands available in Release 12.1.

IPCF is new product for this release.

Command Line Interface

Following new configuration modes and commands added in existing and new CLI configuration modes:

Bulkstats Configuration Mode

- pcc-af schema
- pcc-policy schema
- pcc-quota schema
- pcc-sp-endpt schema
- pcc-service schema

Context Configuration Mode

- event-notif-endpoint
- peer select-peer
- pcc-af-service
- pcc-policy-service
- pcc-service
- pcc-sp-endpoint

Exec Mode Commands

- clear event-notif server
- clear event-notif statistics
- clear pcc-af service
- clear pcc-af session
- clear pcc-policy service statistics
- clear pcc-policy session
- clear pcc-service
- clear pcc-sp-endpoint statistics
- show event-notif server
- show event-notif statistics
- show pcc-af service
- show pcc-af session
- show pcc-policy service
- show pcc-policy session
- show pcc-service
- show pcc-service session
- show pcc-service statistics

- show pcc-sp-endpoint
- show pcc-sp-endpoint connection
- show ipv6

Event-Notification-Interface Endpoint Configuration Mode

- address
- peer name
- peer select-algorithm

PCC-Action-Set Configuration Mode Commands

- af-media-type
- associate monitoring-key
- authorize
- dissociate monitoring-key
- dynamic-rule-install
- dynamic-rule-uninstall
- log-event
- notify-user
- offline-charging-server
- online-charging-server
- request-usage-report monitoring-key
- rule-activate
- rule-deactivate
- rulebase-activate
- rulebase-deactivate
- service-tag
- terminate-session
- usage-monitor

PCC-AF Service Configuration Mode Commands

- associate pcc-service
- diameter dictionary
- diameter origin end-point

PCC-Condition-Group Configuration Mode Commands

- af-application-id
- af-media-codec
- af-media-type
- af-service-urn
- an-gw-address
- authorized-qci

- base-station-id
- bearer-count
- connectivity-access-network
- eval-condition-group
- event-time
- event-trigger
- imsi
- msisdn
- multi-line-or
- nai
- out-of-credit rulename
- out-of-credit rulebase-name
- pcef-address
- pdn-id
- profile-attribute
- radio-access-technology
- rating-group
- sgsn-ip
- sgsn-mcc-mnc
- subscription-attribute
- threshold-condition usage-monitor
- user-access-network
- user-equipment-info

PCC Data Service Configuration Mode Commands

- flow direction
- metering-method
- monitoring-key
- precedence
- qos-profile
- rating-group
- reporting-level
- service-identifier

PCC-Policy Service Configuration Mode Commands

- associate pcc-service
- diameter dictionary
- diameter origin end-point
- ehrpd-access-bcm
- gprs-access-bcm

- max policy-sessions
- subscriber-binding-identifier
- subscription-id-absence-action
- unsolicited-provisioning

PCC-Service-Profile Configuration Mode Commands

- default-rulebase-name
- eval-priority
- service-tag
- usage-monitor
- unknown-services-treatment

PCC-QoS-Profile Configuration Mode Commands

- arp-priority
- guaranteed-bitrate
- max-bitrate
- qci

PCC-Sp-Endpoint Configuration Mode Commands

- access-type
- diameter dictionary
- diameter origin end-point
- diameter peer-select
- profile-data
- profile-update-notification
- spr subscriber identifier

PCC Service Configuration Mode Commands

- action-set
- charging method
- charging server
- condition-group
- data-service
- map-profile priority
- monitoring-key
- multiple-pcef-per-subscriber
- profile
- qos-profile
- spr-failure
- ssc-usage-update-policy
- subscriber-profile

- timedef

PCC-TimeDef Configuration Mode

- start date
- start day
- start time

PCC--Usage-Monitor Configuration Mode

- usage-limit volume

Mobility Management Entity Commands - New in Release 12.0

This section provides information on new MME commands available in Release 12.0.

csfb

The **csfb** command configures Circuit-Switched FallBack options for the configured call control profile. This command sets the CSFB option as only supporting short message service (SMS).

CLI (Call Control Profile Configuration Mode)

```
[ remove ] csfb sms-only
```

lte-policy

This command is a direct replacement for the obsolete **mme-policy** command and contains the same command set as the MME Policy mode.

CLI (Global Configuration Mode)

```
lte-policy
```

nri

The **nri** command configures network resource identifier lengths used for source SGSN discovery via NRI-FQDN based DNS resolution. Up to 8 entries can be configured where each entry specifies the NRI length for a given PLMN.

This change was first introduced in version 12.2, and has since been added to version 12.0.

CLI (MME Service Configuration Mode)

nri length *length* **plmnid mcc** *mcc_value* **mnc** *mnc_value*

IMPORTANT

In the absence of this configuration, the MME treats the NRI as invalid. The MME will use a plain RAI-based FQDN (and not an NRI-based FQDN) for DNS queries made to resolve the source SGSN.

peer-sgsn

This command statically configures peer SGSN environments to facilitate MME-to-SGSN relocations over an S3 or Gn/Gp interface. In prior releases, before this command was created, the MME relied on the DNS setting in the SCTP Service mode for peer SGSN discovery/selection. The order of selection is peer SGSN configuration through MME Service mode first and DNS selection through the SCTP Service mode second.

CLI (MME Service Configuration Mode)

peer-sgsn rai mcc *number* **mnc** *number* **[nri** *value* **] rac** *value* **lac** *value* **address** *ip_address* **capability [gn] [s16] [s3]**

policy inter-rat

This command enables the establishment of indirect data forwarding tunnels for Gn/Gp-based SRNS relocations.

CLI (MME Service Configuration Mode)

policy inter-rat indirect-forwarding-tunnels always

s1-mme ip

This command configures the quality of service QoS differentiated service code point (DSCP) used when sending data packets of a particular 3GPP QoS class over the S1-MME interface.

CLI (MME Service Configuration Mode)

s1-mme ip qos-dscp { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | ef }

sctp-param-template

This command creates a new, or enters an existing SCTP parameter template configuration. SCTP parameter templates configure SCTP associations.

CLI (Global Configuration Mode)

sctp-param-template *name*

This command enters the following mode:

CLI (SCTP Parameter Template Configuration Mode)

The following commands are located in the new SCTP Parameter Template Configuration mode:

sctp-alpha *value*

sctp-alt-accept-flag { disable | enable }

sctp-beta *value*

sctp-checksum-type { adler32 | crc32 }

sctp-cookie-life *value*

sctp-max-assoc-retx *value*

sctp-max-in-strms *value*

sctp-max-init-retx *value*

sctp-max-mtu-size *bytes*

sctp-max-out-strms *value*

sctp-max-path-retx *value*

sctp-min-mtu-size *bytes*

sctp-rto-initial *value*

sctp-rto-max *value*

sctp-rto-min *value*

sctp-sack-frequency *value*

sctp-sack-period { *value* **| units-10ms** *value* **}**

sctp-start-mtu-size *bytes*

timeout { sctp-bundle *value* **| sctp-heart-beat** *value* **}**

timer

To support guarding the Location Update procedure during communication between the SGs service and the VLR, a timer command has been added to the SGS Service mode.

This change was first introduced in version 12.2, and has since been added to version 12.0.

CLI (SGs Service Configuration Mode)

timer ts6-1 *value*

Mobility Management Entity Commands - New in Release 12.2

This section provides information on new MME commands available in Release 12.2.

associate

The **associate** command allows the Diameter endpoint configuration to be associated with SCTP parameters configured in a template.

CLI (Diameter Endpoint Configuration Mode)

associate sctp-parameters-template *template_name*

associate

The **associate** command allows the SGs service to be associated with SCTP parameters configured in a template.

CLI (MME SGs Service Configuration Mode)

associate sctp-param-template *template_name*

diameter-result-code-mapping

The **diameter-result-code-mapping** command allows the administrator to map a specific EMM cause code to an S6a Diameter result code.

CLI (Call Control Profile Configuration Mode)

diameter-result-code-mapping s6a diameter-error-rat-not-allowed mme-emm-cause { no-suitable-cell-in-tracking-area | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }

lai

The **lai** command configures a Local Area Identifier for the management object.

CLI (LTE TAI Management Object Configuration Mode)

lai mcc *number* **mnc** *number* **lac** *area_code*

local-cause-code-mapping

The **local-cause-code-mapping** command maps a selected cause code to a restricted zone code result.

CLI (Call Control Profile Configuration Mode)

local-cause-code-mapping restricted-zone-code emm-cause-code { eps-service-not-allowed-in-this-plmn | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }

lte-emergency-profile

The **lte-emergency-profile** command creates and enters a new LTE Emergency Profile Configuration Mode.

CLI (LTE Policy Configuration Mode)

lte-emergency-profile *name*

The following commands are contained within the new mode:

ambr max-ul *bitrate* **max-dl** *bitrate*

apn *apn_name* **pdn-type (ipv4 | ipv4v6 | ipv6 }**

pgw fqdn *fqdn*

qos qci *qci* **arp** *arp_value* **peemption-capability (may | shall-not } vulnerability (not-preemptable | preemptable)**

ue-validation-level (auth-only | full | imsi | none }

lte-zone-code

The **lte-zone-code** command configures the enforcement of allowed or restricted zone code lists and associates an EMM cause code to rejected attach attempts.

CLI (Call Control Profile Configuration Mode)

```
lte-zone-code [ allow | restrict } { emm-cause-code {
eps-service-not-allowed-in-this-plmn | no-suitable-cell-in-tracking-area |
plmn-not-allowed | roaming-not-allowed-in-this-tracking-area |
tracking-area-not-allowed ] zone-code-list zc_id +
```

msc

The **msc** command configures the IP address of an enhanced Mobile Switching Center (eMSC) server that the MME service communicates with over the Sv interface in support of the Single Radio Voice Call Continuity (SRVCC) feature.

CLI (MME Service Configuration Mode)

```
msc ip_address
```

network-feature-support-ie

The **network-feature-support-ie** command enables the information element in a supported feature message sent by the MME to indicate that Voice over PS is supported.

CLI (Call Control Profile Configuration Mode)

```
network-feature-support-ie ims-voice-over-ps
```

network-global-mme-id-mgmt-db

The **network-global-mme-id-mgmt-db** command creates and enters a new LTE Network Global MME ID Management Database Configuration Mode.

CLI (LTE Policy Configuration Mode)

```
network-global-mme-id-mgmt-db
```

The following commands are contained within the new mode:

plmn

network-sharing

To support a network sharing configuration where service providers can share core network elements (MME, SGW, PGW), the MME service can now be configured with multiple local PLMNs per service. The configuration of these additional PLMNs is implemented using the **network-sharing** command within the mme-service config mode.

Refer to the **plmn-id** command to create the base PLMN identifier for an MME service. Each PLMN ID consists of the Mobile Country Code (MCC) and Mobile Network Code (MNC). A maximum of four network sharing entries can be configured per MME service. These PLMN IDs will be communicated to the eNodeBs in the S1 SETUP response and MME CFG Update messages.

CLI (MME Service Configuration Mode)

network-sharing plmnid mcc *number* **mnc** *number* **mme-id group-id** *id* **mme-code** *code*

nri

The **nri** command configures network resource identifier lengths used for source SGSN discovery via NRI-FQDN based DNS resolution. Up to 8 entries can be configured where each entry specifies the NRI length for a given PLMN.

CLI (MME Service Configuration Mode)

nri length *length* **plmnid mcc** *mcc_value* **mnc** *mnc_value*

IMPORTANT

In the absence of this configuration, the MME treats the NRI as invalid. The MME will use a plain RAI-based FQDN (and not an NRI-based FQDN) for DNS queries made to resolve the source SGSN.

plmn-id

To support enhanced TAI to LAI mapping, the **plmn-id** command has been added to support the optional configuration of the Public Land Mobile Network (PLMN) ID to identify the LAC pool area.

CLI (MME LAC Pool Area Configuration Mode)

plmn-id mcc *mcc_value* **mnc** *mnc_value*

timer

To support guarding the Location Update procedure during communication between the SGs service and the VLR, a timer command has been added to the SGS Service mode.

CLI (SGs Service Configuration Mode)

timer ts6-1 *value*

timezone

The **timezone** command configures the timezone to be used for the UE time zone in S11 and NAS messages.

CLI (LTE TAI Management Object Configuration Mode)

timezone { + | - } hours *value* **[minutes (0 | 15 | 30 | 45]**

zone-code

The **zone-code** command configures a zone code for the management object.

CLI (LTE TAI Management Object Configuration Mode)

zone-code *zc_id*

NAT Commands - New in Release 12.0

This section provides information on new NAT commands available in Release 12.0.

h323 time-to-live

This command configures registration lifetime to maintain NAT binding.

CLI (ACS Configuration Mode)

h323 time-to-live *timeout*

default h323 time-to-live

h323 timeout

This command configures the timeout interval for H323 requests.

CLI (ACS Configuration Mode)

h323 timeout { admission *adm_timeout* | **discovery** *disc_timeout* | **location** *loc_timeout* | **registration** *reg_timeout* | **unregistration** *unreg_timeout* **}**

default h323 timeout { admission | discovery | location | registration | unregistration }

h323 tpkt

This command configures the Transport Protocol Data Unit Packet (TPKT).

CLI (ACS Configuration Mode)

h323 tpkt *timeout*

default h323 tpkt

h323 version

This command configures the supported H323 versions.

CLI (ACS Configuration Mode)

h323 version *version_num*

default h323 version

NAT Commands - New in Release 12.2

This section provides information on new NAT commands available in Release 12.2.

icsr-flow-recovery

This command enables/disables the NAT ICSR Flow check-pointing support for subscribers in a Firewall-and-NAT policy.

CLI (Firewall-and-NAT Access Ruledef Configuration Mode)

[default | no] nat icsr-flow-recovery

ip server-ipv6-network-prefix

This command configures an access ruledef to analyze user traffic based on IPv6 server prefix.

CLI (Firewall-and-NAT Access Ruledef Configuration Mode)

[no] ip server-ipv6-network-prefix *operator ipv6_prefix/maskbit*

Packet Data Network Gateway Commands - New in Release 12.0

This section provides information on new P-GW commands available in Release 12.0.

action

This command configures the action priority for an actiondef.

CLI (Local Policy Actiondef Configuration Mode)

action priority *priority action_name arguments*

no action priority *priority*

actiondef

This command enables creating, configuring, or deleting action definitions within a local policy service.

CLI (Local Policy Service Configuration Mode)

actiondef *actiondef_name* **[-noconfirm]**

no actiondef *actiondef_name*

This command enters the following mode:

CLI (Local Policy Actiondef Configuration Mode)

The following commands are located in the new Local Policy Actiondef Configuration mode:

action priority *priority action_name arguments*

end

exit

allocation-retention-priority

This command configures the Allocation Retention Priority (ARP).

CLI (ACS Charging Action Configuration Mode)

allocation-retention-priority *priority* **[pci** *value* **|** **pvi** *value* **]**

no allocation-retention-priority

condition

This command is used to configure the conditions which trigger the ruledef event.

CLI (Local Policy Ruledef Configuration Mode)

condition priority *priority* **{** *variable* **{ eq | ge | gt | le | lt | match | ne | nomatch }** *regex* | *string_value* | *int_value* | *set* **}**

no condition priority *priority*

eventbase

This command enables creating, configuring, or deleting an event base within a local policy service.

CLI (Local Policy Service Configuration Mode)

eventbase *eventbase_name* **[-noconfirm]**

no eventbase *eventbase_name*

This command enters the following mode:

CLI (Local Policy Eventbase Configuration Mode)

The following commands are located in the new Local Policy Eventbase Configuration mode:

end

exit

rule priority *priority* **[event** *list_of_events* **] ruledef** *ruledef_name* **actiondef** *actiondef_name* **[continue]**

local-policy-service

This command enables creating, configuring, or deleting a local QoS policy.

CLI (Global Configuration Mode)

local-policy-service *name* **[-noconfirm]**

This command enters the following mode:

CLI (Local Policy Service Configuration Mode)

The following commands are located in the new Local Policy Service Configuration mode:

actiondef *actiondef_name* **[-noconfirm]**

eventbase *eventbase_name* **[-noconfirm]**

end

exit

ruledef *ruledef_name* **[-noconfirm]**

mobility-option-type-value

This command changes the mobility option type value used in mobility messages.

CLI (LMA Service Configuration Mode)

mobility-option-type-value { custom1 | standard }

default mobility-option-type-value

permission

This command enables the ability to use network mobility service (NEMO) for the current APN. NEMO is disabled by default.

CLI (APN Configuration Mode)

[no] permission nemo

default permission

policy

This command configures the Mobile IPv6 policy to decide on action to be taken when IPv4/IPv6 subscriber packets need to be tunneled, however, the encapsulated packets exceed tunnel MTU size.

CLI (APN Configuration Mode)

policy ipv6 tunnel mtu exceed { fragment [inner] | notify-sender }

[default | no] policy ipv6 tunnel mtu exceed

rule

This command enables the setting of event rules. An event is something that occurs in the system which would trigger a set of actions to take place, such as new-call or rat-change.

CLI (Local Policy Eventbase Configuration Mode)

rule priority *priority* **[event** *list_of_events* **] ruledef** *ruledef_name* **actiondef** *actiondef_name* **[continue]**

no rule priority *priority*

ruledef

This command enables creating, configuring, or deleting a rule definition within a local policy service.

CLI (Local Policy Service Configuration Mode)

ruledef *ruledef_name* **[-noconfirm]**

no ruledef *ruledef_name*

This command enters the following mode:

CLI (Local Policy Ruledef Configuration Mode)

The following commands are located in the new Local Policy Ruledef Configuration mode:

condition priority *priority* **{** *variable* **{ eq | ge | gt | le | lt | match | ne | nomatch }** *regex* | *string_value* | *int_value* | *set* **}**

end

exit

signalling-packets

This command enables the DSCP marking feature for IP headers carrying outgoing signalling packets.

CLI (LMA Service Configuration Mode)

signalling-packets ip-header-dscp *value*

[default | no] signalling-packets ip-header-dscp

Packet Data Network Gateway Commands - New in Release 12.2

This section provides information on new P-GW commands available in Release 12.2.

accounting-keys

This command aggregates the accounting information, using the configurable keys (qci) along with default keys.

CLI (Accounting Policy Configuration Mode)

accounting-keys qci

default accounting-keys

emergency-apn

This command configures APN as an emergency APN for VoLTE based E911 support.

CLI (APN Configuration Mode)

[default | no] emergency-apn

p-cscf

This command enables use of locally configured P-CSCF addresses or Fully Qualified Domain Name (FQDN).

CLI (APN Configuration Mode)

p-cscf { fqdn *fqdn* **| primary [ip** *IPv4_address* **| ipv6** *IPv6_address* **] | secondary [ip** *IPv4_address* **| ipv6** *IPv6_address* **] }**

no p-cscf { fqdn | primary [ip | ipv6] | secondary [ip | ipv6] }

sequence-number

This command enables addition of the sequence number to every GTP-U packet. Default is disabled.

CLI (GTP-U Service Configuration Mode)

[no] sequence-number

timeout emergency-inactivity

This command configures the emergency session inactivity-timeout for an APN. APN must be configured as an emergency APN for VoLTE based E911 support.

CLI (APN Configuration Mode)

timeout emergency-inactivity *seconds*

[default | no] timeout emergency-inactivity

PDIF Commands - New in Release 12.0

This section provides information on new PDIF commands available in Release 12.0.

None for this release.

PDSN Commands - New in Release 12.0

This section provides information on new PDSN commands available in Release 12.0.

bgp

The following command has been added.

- bgp extended-asn-cap

CLI (Context Configuration Mode)

[no] bgp extended-asn-cap

maximum-paths ebgp

The following command has been added.

- maximum-paths ebgp

CLI (Router Bgp Mode)

maximum-paths ebgp *value*

[no] maximum-paths ebgp

a11-signalling-packets

The following command is added.

- a11-signalling-packets

CLI (Pdsn-service Mode)

a11-signalling-packets ip-header-dscp *value*

[no | default] a11-signalling-packets ip-header-dscp

fa-spi-list / ha-spi-list

The following commands are added.

- fa-spi-list
- ha-spi-list

CLI (Config Mode)

fa-spi-list *list*

ha-spi-list *list*

aaa nas-ip-address *IPv4*

The following commands are added.

- aaa nas-ip-address IPv4
- aaa 3gpp2-service-option

CLI (PDSN Service Config Mode)

aaa nas-ip-address *ip-address*

aaa 3gpp2-service-option *service option*

show ipv6 ospf

Following command shows ipv6 ospf options and its results.

CLI (Context Configuration Mode)

show ipv6 ospf [database [adv-router *IPv4-Address* **] [ls-type { external | inter-prefix | inter-router | intra-prefix | link | network | router }] [verbose] [| { grep** *grep_options* **| more }]] [debugging] [interface] [neighbor [details]] [route [summary]] [virtual-links] [| { grep** *grep_options* **| more }]**

Serving Gateway Commands - New in Release 12.0

This section provides information on new commands available in Release 12.0.

apn-profile

The S-GW now supports the use of the APN Profile Configuration Mode commands. The **apn-profile** *name* command is located in the Global Configuration Mode.

CLI (APN Profile Configuration Mode)

The following commands in this mode are supported by the S-GW:

cc { local-value-for-scdrs behavior *bit_value* **profile** *index_bit* **| prefer { hlrvalue-for-scdrs | local-value-for-scdrs } }**

description *description*

idle-mode-acl { ipv4 | ipv6 } access-group *group_name*

ip { qos-dscp { { downlink | uplink } { background *forwarding* **| conversational** *forwarding* **| interactive traffic-handling-priority** *priority_forwarding* **| streaming** *forwarding* **} + } | source-violation { deactivate [all-pdp | excludefrom accounting | linked-pdp | tolerance-limit } | discard [exclude-fromaccounting] | ignore }**

call-control-profile

The S-GW now supports the use of the Call Control Profile Configuration Mode commands. The **call-control-profile** *name* command is located in the Global Configuration Mode.

CLI (Call Control Profile Configuration Mode)

The following commands in this mode are supported by the S-GW:

attach access-type { gprs | umts } { all | location-area-list instance *list_id* **}{ failure-code** *code* **| user-device-release { before-r99 failure code** *code* **| r99-or-later failure code** *code* **}**

attach allow access-type { eps | gprs | umts } location-area-list instance *list_id*

attach restrict access-type { eps | gprs | umts } { all | location-area-list instance *list_id* **}**

attach imei-query-type { imei | imei-sv | none } [[verify-equipment-identity] [deny-greylisted]

attach imei-query-type

authenticate { activate [access-type { gprs | umts }] | first [access-type { gprs | umts }] | frequency *frequency* **| primary [access-type { gprs | umts }] | all-events [access-type { gprs | umts } | frequency** *frequency* **| attach [access-type { gprs | umts } | attach-type { combined | gprs-only } [access-type { gprs | umts } | frequency frequency] | frequency** *frequency* **| inter-rat [access-type { gprs | umts }]] | detach [access-type { gprs | umts }] | rau | service-request | sms | tau }**

description *description*

equivalent-plmn radio-access-technology { 2G | 3g | 4g | any } plmnid mcc *mcc_number mnc_number* **priority** *priority*

treat-as-hplmn

operator-policy

The S-GW now supports the use of the Operator Policy Configuration Mode commands. The **operator-policy** *name* command is located in the Global Configuration Mode.

CLI (Operator Policy Configuration Mode)

The following commands in this mode are supported by the S-GW:

apn { default-apn-profile *apn_profile_name* **| network-identifier** *apn_net_id* **apn-profile** *apn_profile_name* **| operator-identifier** *apn_op_id* **apn-profile** *apn_profile_name* **}**

associate { apn-remap-table *table_id* **| call-control-profile** *profile_id* **}**

description *description*

imei range *IMEI_number* **to** *IMEI_number* **{ imei-profile** *profile_name* **| sv ## imeiprofile** *profile_name* **}**

lte-policy

This command is a direct replacement for the obsolete **mme-policy** command and contains the same command set as the MME Policy mode. The S-GW now supports the following modes in the LTE Policy Configuration Mode: LTE Subscriber Map Configuration Mode and LTE TAI Management Database Configuration Mode.

CLI (Global Configuration Mode)

lte-policy

Serving Gateway Commands - New in Release 12.2

This section provides information on new commands available in Release 12.2.

ddn

Sets a timer that delays the sending of excess Downlink Data Notification messages by the S-GW to the MME in instances where downlink data is received before a Modify Bearer Request is received by the MME.

CLI (S-GW Service Configuration Mode)

ddn failure-action pkt-drop-time *seconds*

sequence-number

This command enables addition of the sequence number to every GTP-U packet. Default is disabled.

CLI (GTP-U Service Configuration Mode)

[no] sequence-number

Session Control Manager Commands - New in Release 12.0

This section provides information on new SCM commands available in Release 12.0.

bgcf-proxy

This command enables SIP BGCF proxy for the service.

CLI (CSCF Proxy-CSCF Configuration Mode)

bgcf-proxy [port *value* **| transport { tcp | udp } port** *value* **]**

[default | no] bgcf-proxy

core-reg-expiry-time

This command configures Registration Expiry Timer Handling in P-CSCF/A-BG to keep pin holes open in B2BUA mode.

CLI (CSCF Proxy-CSCF Configuration Mode)

core-reg-expiry-time *sec*

[default | no] core-reg-expiry-time

emergency-call-mode

This command enables the P-CSCF/A-BG service to add “P-Emergency-Call-Mode-Preference” header in 200OK to REGISTER message. By default, this command is disabled.

CLI (CSCF Proxy-CSCF Configuration Mode)

emergency-call-mode { 3gpp-cs | 3gpp-ims }

[default | no] emergency-call-mode

lawful-intercept

This command enables Lawful Intercept (LI) in this CSCF service. Feature is disabled by default.

CLI (CSCF Service Configuration Mode)

[no] lawful-intercept

pcrf-policy-control

This command enables external policy control via PCRF through the Rx Diameter interface and enters the PCRF-Policy-Control Configuration Mode. Default is disabled.

CLI (Proxy-CSCF Configuration Mode)

[no] pcrf-policy-control

This command enters the following mode:

CLI (CSCF PCRF-Policy-Control Configuration Mode)

The following commands are located in the new PCRF-Policy-Control Configuration Mode:

[no] authorization mediatype { application | audio | control | data | message | others | text | video }

end

exit

[no] signaling-bearer-loss subscription

signaling-bearer-loss

This command replaces the **subscribe** command in the CSCF Proxy-CSCF Configuration Mode. Use this command to enable subscription to Notification of Signaling Transmission Path Status, as well as IPCAN Change type notification.

When enabled (default), the P-CSCF/A-BG sends AAR to the external PCRF via the Rx interface after UE registration. When disabled, the P-CSCF/A-BG will not subscribe to any event during Registration with PCRF and no diameter session will be established.

CLI (CSCF PCRF-Policy-Control Configuration Mode)

[no] signaling-bearer-loss subscription

ca-certificate

This command specifies a list of ca-certificates.

CLI (SSL Template Configuration Mode)

ca-certificate list *name*

certificate

This command is used to bind an X.509 trusted certificate to the SSL template.

CLI (SSL Template Configuration Mode)

certificate *name*

cipher-suite

This command creates a new SSL cipher suite or specifies an existing cipher suite and enters the Cipher Suite Configuration Mode.

CLI (Context Configuration Mode)

[no] cipher-suite *name*

This command enters the following mode:

CLI (Cipher Suite Configuration Mode)

The following commands are located in the new Cipher Suite Configuration mode:

encryption { 3des | aes-128 | null | rc4 }

end

exit

hmac { sha1 }

key-exchange { rsa }

cipher-suites

This command specifies a list of SSL cipher suites. Currently, the system supports only one SSL cipher suite per SSL template.

CLI (SSL Template Configuration Mode)

cipher-suites list *name*

clear ssl statistics

This command deletes all previously gathered SSL statistics for a specific P-CSCF service or all P-CSCF services, either system-wide or within a context.

CLI (Exec Mode)

clear ssl statistics [service-name *name* **]**

encryption

This command specifies the encryption algorithm for the SSL cipher suite.

CLI (Cipher Suite Configuration Mode)

encryption { 3des | aes-128 | null | rc4 }

default encryption

hmac

This command specifies the HMAC (keyed-Hash Message Authentication Code) for the SSL cipher suite.

The default and only currently available option is SHA-1 (Secure Hash Algorithm-1).

CLI (Cipher Suite Configuration Mode)

hmac { sha1 }

default hmac

key-exchange

This command specifies the key exchange algorithm for the SSL cipher suite. The key exchange algorithm provides the means by which the cryptographic keys for conventional encryption and MAC calculations are exchanged.

The default and only currently available option is RSA (Rivest, Shamir, and Adleman).

CLI (Cipher Suite Configuration Mode)

key-exchange { rsa }

default key-exchange

require cipher ssl resource-percentage

This command assigns the 8 processing cores on the PSC2 card and splits the hardware acceleration resources between SSL protocol and IPSec protocol processing.

CLI (Global Configuration Mode)

require cipher ssl resource-percentage *percentage_value*

default require cipher ssl resource-percentage

show ssl cipher-suite

This command displays information related to SSL cipher suites since the last restart or clear command. A cipher suite contains the cryptographic algorithms supported by the client.

CLI (Exec Mode)

show ssl cipher-suite [name *name* **] [| { grep** *grep_options* **| more }]**

show ssl connection

This command displays information pertaining to SSL connections on the P-CSCF.

CLI (Exec Mode)

show ssl connection [list | summary [service-name *name* **]] [name** *name* **] [| { grep** *grep_options* **| more }]**

show ssl map

This command displays information related to configured SSL maps/templates since the last restart or clear command.

CLI (Exec Mode)

show ssl map [map-type ssl-subscriber-template] [name *name* **] [| { grep** *grep_options* **| more }]**

show ssl statistics

This command displays statistics for SSL since the last restart or clear command.

CLI (Exec Mode)

show ssl statistics [service-name *name* **] [| { grep** *grep_options* **| more }]**

ssl

This command creates a new SSL template or specifies an existing one and enters the SSL Template Configuration Mode.

CLI (Context Configuration Mode)

[no] ssl template *name* **{ ssl-subscriber }**

This command enters the following mode:

CLI (SSL Template Configuration Mode)

The following commands are located in the new SSL Template Configuration mode:

ca-certificate list *name*

certificate *name*

cipher-suites list *name*

end

exit

version list { tlsv1 }

version

This command specifies the supported version(s) of SSL protocol on the P-CSCF/A-BG. Currently, there is only one supported version of SSL protocol, which is TLS v0.1.

CLI (SSL Template Configuration Mode)

version list { tlsv1 }

default version

Session Control Manager Commands - New in Release 12.2

This section provides information on new SCM commands available in Release 12.2.

aaa-group

This command configures matching criteria for selecting a aaa-group name. When a subscriber registers, the selection criteria are compared and the aaa-group name from the matching entry will be picked up. The selected aaa-group will be used for all CDF (enabled for a given access type) or HSS interactions for that subscriber.

Maximum of 3 criteria can be configured per entry. A maximum of 1024 such entries can be configured.

CLI (CSCF Diameter Selection Configuration Mode)

aaa-group *name* **{ [preference** *value* **] criteria { aor** *aor_prefix* **|** **subscriber-capability {** *capability_type* **} | subscriber-ip-type** **{ v4 | v6 } } + }**

no aaa-group *name* **preference** *value*

as-call

This command enables or disables the update of AS Call related Invite Request URI with translation result in the CSCF service.

CLI (CSCF Serving-CSCF Configuration Mode)

[default | no] as-call invite-request-uri update

authorization policy-interworking-failure

This command allows/rejects a call based on configuration in case of failure from PCRF. By default, session-reject is activated to reject the call with default response code 500.

CLI (CSCF PCRF-Policy-Control Configuration Mode)

authorization policy-interworking-failure { session-continue | **session-reject [response-code** *code* **] }**

default authorization policy-interworking-failure

bind

This command binds the NPDB client to an IP address or domain, port, and password.

CLI (CSCF NPDB Client Configuration Mode)

bind address *IPv4_address* **system-id** *system_id* **id** *client_id* **{ encrypted** **password** *password* **| password** *password* **}**

no bind

caller-preference

This command enables or disables custom SIP caller preferences.

CLI (CSCF Service Configuration Mode)

caller-preference custom

[default | no] caller-preference

cscf diameter-selection

This command creates a CDF or HSS selection table and enters the CSCF Diameter Selection Configuration Mode.

When HSS table has entries, this criteria is always applied for HSS server selection.

CDF server selection can be enabled or disabled for a given access type.

CLI (Context Configuration Mode)

cscf diameter-selection type { cdf | hss } [-noconfirm]

no cscf diameter-selection type { cdf | hss }

This command enters the following mode:

CLI (CSCF Diameter Selection Configuration Mode)

The following commands are located in the new CSCF Diameter Selection Configuration Mode:

aaa-group *name* **{ [preference** *value* **] criteria { aor** *aor_prefix* **| subscriber-capability {** *capability_type* **} | subscriber-ip-type { v4 | v6 } } + }**

no aaa-group *name* **preference** *value*

end

exit

cscf peer-servers-group

This command creates a peer server group and enters the Peer Servers Group Configuration Mode.

CLI (Context Configuration Mode)

cscf peer-servers-group *group_name* **type sip-as [-noconfirm]**

no cscf peer-servers-group *group_name*

This command enters the following mode:

CLI (CSCF Peer Servers Group Configuration Mode)

The following commands are located in the new CSCF Peer Servers Group Configuration Mode:

end

exit

[no] peer-servers *server_name*

cscf prefix-table

This command creates a prefix table and enters the Prefix Table Configuration Mode.

CLI (Context Configuration Mode)

[no] cscf prefix-table

This command enters the following mode:

CLI (CSCF Prefix Table Configuration Mode)

The following commands are located in the new CSCF Prefix Table Configuration Mode:

end

exit

number *number* **[ported] [routing-domain** *domain* **]**

custom reg-binding

This command controls whether the S-CSCF returns only one or all bindings for AOR in 200 OK REGISTER response.

CLI (CSCF Service Configuration Mode)

[no] custom reg-binding

custom response

This command configures reject with specific response code for UE capability failure.

CLI (CSCF Service Configuration Mode)

custom response ue-capability-failure { *capability_type* **} reject response-code {** *response_code* **}**

no custom-response ue-capability-failure { *capability_type* **}**

custom volte

This command enables custom features. By default, this command is disabled.

CLI (CSCF Service Configuration Mode)

[default | no] custom volte

diameter-selection

This command enables or disables prefix and capability based CDF server selection. By default, this command is disabled.

CLI (CSCF Access Profile Configuration Mode)

[no] diameter-selection cdf

dummy-as

This command sets a response code for Dummy-AS. If this mode is selected, then MESSAGE/PUBLISH requests will be responded to by S-CSCF with configured response code. The response code can be 2xx/4xx/5xx/6xx; 3xx,401,and 407 are not allowed.

CLI (CSCF Peer Server Monitoring Configuration Mode)

dummy-as custom-response-code *SIP_response_code*

default dummy-as custom-response-code

forking

This command controls the default-request forking-type in S-CSCF. The default forking type is parallel.

CLI (CSCF Serving-CSCF Configuration Mode)

forking { parallel | serial }

[default | no] forking

multiple-reg

This command allows multiple registrations for the same private user-id from different devices. By default, multiple registrations are not allowed for the same private user-id.

CLI (CSCF Service Configuration Mode)

[default | no] multiple-reg same-private-id

npdb-client

This command creates an NPDB (Number Portability Data Base) client and enters the CSCF NPDB Client Configuration Mode.

CLI (CSCF Serving-CSCF Configuration Mode)

npdb-client *client_name* **[-noconfirm]**

[no] npdb-client

This command enters the following mode:

CLI (CSCF NPDB Client Configuration Mode)

The following commands are located in the new CSCF Prefix Table Configuration Mode:

bind address *IPv4_address* **system-id** *system_id* **id** *client_id* **{ encrypted password** *password* **| password** *password* **}**

no bind

end

exit

npdb-primary-server { address *IPv4_address* **| domain** *domain* **} port** *port_number*

no npdb-primary-server

npdb-secondary-server { address *IPv4_address* **| domain** *domain* **} port** *port_number*

no npdb-secondary-server

timeout { bind-response secs | error-response secs | idle secs | ping secs | ping-response secs | query-response secs | release-response secs | tcp-retry secs }

[default | no] timeout { bind-response | error-response | idle | ping | ping-response | query-response | release-response | tcp-retry }

npdb-primary-server

This command configures the NPDB primary server.

CLI (CSCF NPDB Client Configuration Mode)

npdb-primary-server { address *IPv4_address* **| domain** *domain* **} port** *port_number*

no npdb-primary-server

npdb-secondary-server

This command configures the NPDB secondary server.

CLI (CSCF NPDB Client Configuration Mode)

npdb-secondary-server { address *IPv4_address* **| domain** *domain* **} port** *port_number*

no npdb-secondary-server

number

This command determines for each number (or number prefix) in a prefix table whether it is ported and the SIP routing domain.

CLI (CSCF Prefix Table Configuration Mode)

number *number* **[ported] [routing-domain** *domain* **]**

no number *number*

pcrf-policy-control

This command enables or disables PCRF policy control for this access-type. By default, PCRF policy control is disabled.

CLI (CSCF Access Profile Configuration Mode)

[default | no] pcrf-policy-control

peer-servers

This command configures peer-server lists in a peer-servers-group. The peer-servers-list can be active, standby, or default.

Note: There can be one active, one standby, and one default peer-servers-list in a peer-servers-group.

CLI (CSCF Peer Servers Group Configuration Mode)

peer-servers *server_name* **{ default | mode { active | standby } }**

[no] peer-servers *server_name*

psap-file

This command sets the location of the PSAP-Database file to maintain and access the ESRK-Ranges provided by the operator for the E-CSCF.

CLI (CSCF Emergency-CSCF Configuration Mode)

psap-file *file_name*

no psap-file

redirect

This command configures the system to redirect subscriber sessions to another CSCF based on criteria(s) matching the received packet.

CLI (CSCF ACL Configuration Mode)

redirect { address *ip_address* | **host** *host_name* **} [port** *port_number* **] { any** | **destination aor** *aor* | **log { any** | **destination aor** *aor* | **source { address** *ip_address* | **aor** *aor* **} | subscriber-capability {** *capability_type* **} | user-agent device-type** *device_type* **} | source { address** *ip_address* | **aor** *aor* **} | subscriber-capability {** *capability_type* **} | user-agent device-type** *device_type* **+ }**

no redirect { address *ip_address* | **host** *host_name* **} [port** *port_number* **] { any** | **destination aor** *aor* | **source { address** *ip_address* | **aor** *aor* **} | subscriber-capability {** *capability_type* **} | user-agent device-type** *device_type* **+ }**

registration

This command specifies whether the S-CSCF skips third party registration to the Application Server (AS) by a configured time after initial registration. After skipping the configured number of times, the third party register should be sent again to AS to reduce overload on AS. By default, the registration skip count is zero.

CLI (CSCF Peer Server Monitoring Configuration Mode)

registration skip-count *count*

no registration skip-count

RetryAfter-header-value

This command sets the minimum and maximum value in seconds for Retry-After Header. If Transactions Per Second (TPS) rate towards the peer-server application server (AS) is exceeded, the incoming requests will be rejected with 500 error response; Retry-After Header specifies the number of seconds before UE should retry.

CLI (CSCF Service Configuration Mode)

RetryAfter-header-value min-value *secs* **max-value** *secs*

default RetryAfter-header-value

server-name

This command enables/disables filling the server name AVP in MAR and SAR for Cx interface with configured server name. This command is disabled by default.

CLI (CSCF Serving-CSCF Configuration Mode)

server-name *server_name*

no server-name

strict-check

This command enables strict checking on default-aor-domain so S-CSCF will reject registration and invite if there is a mismatch between aor in To/From and the configured default-aor-domain. By default, strict checking on default-aor-domain is disabled.

CLI (CSCF Service Configuration Mode)

[default | no] strict-check configured-aor-domain

timeout

This command configures timeout values for NPDB client.

CLI (CSCF NPDB Client Configuration Mode)

timeout { bind-response *secs* **| error-response** *secs* **| idle secs | ping** *secs* **| ping-response** *secs* **| query-response** *secs* **| release-response** *secs* **| tcp-retry** *secs* **}**

[default | no] timeout { bind-response | error-response | idle | ping | ping-response | query-response | release-response | tcp-retry }

tps-rate

This command controls the Transactions Per Second (TPS) towards the peer-server application server (AS). If TPS rate is exceeded, the incoming requests will be rejected with 500 error response; Retry-After Header specifies the number of seconds before UE should retry.

CLI (CSCF Peer Server Monitoring Configuration Mode)

tps-rate *rate* **[exclude Register]**

no tps-rate

user-authorization

If this command is enabled, and I-CSCF role is enabled in S-CSCF, I-CSCF will send UAR/UAA diameter message to HSS.

CLI (CSCF Serving-CSCF Configuration Mode)

[default | no] user-authorization

SGSN Commands - New in Release 12.0

This section provides information on new SGSN commands available in Release 12.0.

access-restriction-data

This new command enables the operator to assign a failure code to be included in reject messages if attach rejection is due to access restriction data (ARD) checking in incoming subscriber data (ISD) messages. As well, the operator can disable the ARD checking behavior.

CLI (Call Control Profile Configuration Mode)

access-restriction-data { failure-code *cause_code* **| no-check }**

remove access-restriction-data failure-code

aggregate-ipc-msg

New command enables/disables aggregation of IPC messages in linkmgr and sessmgr.

CLI (SGSN-Global Configuration Mode)

aggregate-ipc-msg { linkmgr | sessmgr } { flush-frequency *frequency* **| num-msgs** *number_msgs* **}**

default aggregate-ipc-msg { linkmgr | sessmgr }

apn-resolve-dns-query snaptr

This new command enables the SGSN to send an straightforward name authority pointer (SNAPTR) type DNS query for APN resolution. The SNAPTR filters based on the EPC-capability of the user equipment (UE).

CLI (SGSN-Global Configuration Mode)

[default | no] apn-resolve-dns-query snaptr

associate-dscp-template

This new command in the GPRS Service configuration mode associates a specific DSCP template with a specific GPRS service configuration.

CLI (GPRS Service Configuration Mode)

associate-dscp-template downlink *template_name*

no associate-dscp-template downlink

bssgp-message

A new command determines the SGSN response to MS-Flow-Control messages received from an unknown MS.

CLI (SGSN Global Configuration Mode)

bssgp-message ms-flow-control-from-unknown-ms { discard-message | send-ack | send-status }

[default] bssgp-message ms-flow-control-from-unknown-ms

check-zone-code

Command enables/disables a mechanism to check zone codes.

CLI (Call-Control Profile Configuration Mode)

[no | remove] check-zone-code

check-imei

New commands determine the SGSN's action during an attach process if the route towards the EIR is down.

IMPORTANT

The **`check-imei gf-failure-action`** command described below for 2G and 3G SGSNs works only if the EIR is associated under map-service and the EIR link is down. If **`check-imei gf-failure-action`** is configured as **`continue`**, and there is no EIR associated under map-service, then the SGSN rejects the Attach procedure with the disconnect-reason c*heck-imei failure.*

CLI (SGSN-Service Configuration Mode & GPRS Service Configuration Mode)

```
[ default ] check-imei { gf-failure-action | gf-timeout-action } { continue
| reject }
```

control-packet

This command in the new DSCP template mode configure handling of downlink control packets.

CLI (DSCP Template Configuration Mode)

```
control-packet qos-dscp { af11 | af12 | af13 | af21 | af22 | af23 | af31 |
af32 | af33 | af41 | af42 | af43 | be | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 |
cs7 | ef }]
```

```
default control-packet
```

data-packet

This command in the new DSCP template mode configure handling of downlink data packets.

CLI (DSCP Template Configuration Mode)

```
data-packet { background | conversational | interactive { priority1 |
priority2 | priority3 } | streaming } qos-dscp { af11 | af12 | af13 | af21
| af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | cs1 | cs2 |
cs3 | cs4 | cs5 | cs6 | cs7 | ef }]
```

```
default data-packet { background | conversational | interactive { priority1
| priority2 | priority3 } | streaming }
```

disable-remote-restart-counter-verification

This new command disables the SGSN's default behavior for verification of remote peer's restart counter change values.

CLI (SGTP Service Configuration Mode)

```
[ no | default ] disable-remote-restart-counter-verification
```

dlci-util schema

A new command has been added to the Bulkstats configuration mode to configure bulk statistics collection for the DLCI utilization:

CLI (Bulkstats Configuration Mode)

```
[ no ] dlci-util schema <dlci_schema_name> format <dlci_schema_format>
```

dscp-template

Use this new command to create or delete DSCP templates and to gain to the new DSCP templates configuration mode. The new DSCP template mode provides commands to configure control and data-packet handling:

- **control-packet** command configures DSCP values for downlink control packets
- **data-packet** command configures DSCP values for downlink data packets

CLI (SGSN Global Configuration Mode)

[no] dscp-template *template_name* **[-noconfirm]**

empty-cr

This new command allows the operator to enable a feature which determines how empty (no data parameters) Connection Request messages will be handled.

CLI (IuPS Service Configuration Mode)

[default | no] empty-cr procedure reject

ggsn-fail-retry-timer

Sets the amount of time that a GGSN will be unavailable/blacklisted.

CLI (SGTP Service Configuration Mode)

ggsn-fail-retry-timer *value*

no ggsn-fail-retry-timer

gmm-message

The new command configures the SGSN to discard (drop) the Attach-Request message received with a random TLLI already in use.

CLI (SGSN-Global Configuration Mode)

[default] gmm-message attach-with-tlli-in-use discard-message

gn-delay-monitoring

New command enables monitoring of the delay of packets over Gn/Gp between the SGSN and GGSN.

CLI (SGTP Service Configuration Mode)

gn-delay-monitoring [num-delay *number_delayed* **| num-no-delay-for-clear** *number_normal* **| tolerance-seconds** *number_seconds* **]**

default gn-delay-monitoring [num-delay | num-no-delay-for-clear | tolerance-seconds]

no gn-delay-monitoring

local-cause-code-mapping

New command allows the operator to determine the GMM reject cause code to be sent to the UE for map-cause ‘roaming not allowed’; options include:

- gprs-serv-and-non-gprs-serv-not-allowed
- gprs-serv-not-allowed
- gprs-serv-not-in-this-plmn
- location-area-not-allowed
- network-failure
- no-suitable-cell-in-this-la
- plmn-not-allowed
- roaming-not-allowed-in-this-la

IMPORTANT

When mapping is configured, CLI-mapping overrides private ext information for access type in situations involving ‘roaming-not-allowed’ map cause

CLI (Call-Control-Profile Configuration Mode)

local-cause-code-mapping map-cause-code roaming-not-allowed gmm-cause-code <gmm-cause>

remove local-cause-code-mapping map-cause-code roaming-not-allowed

max-remote-restart-counter-change

This command sets a restart counter change window to avoid the resulting service deactivations and activations causing large bursts of network traffic if the restart counter change messages from the GGSN are erroneous.

CLI (SGTP Service Configuration Mode)

max-remote-restart-counter-change <*value 1 - 255***>**

default max-remote-restart-counter-change

map-message

A new configuration command instructs the SGSN to either ignore or validate the CAMEL subscription when there is no CAMEL service associated or in existence.

CLI (SGSN-Global Configuration Mode)

map-message insert-subscriber-data csi-handling when-camel-not-associated ignore-subscription

default map-message insert-subscriber-data csi-handling

min-unused-auth-vector

A new configuration command defines a threshold for the minimum number of unused vectors that the SGSN will retain before triggering the initiation of a SAI.

CLI (Call-Control Profile Configuration Mode)

min-unused-auth-vector <*min#_vectors***>**

remove min-unused-auth-vector

mtp2-max-outstand-frames

A new command provides a new default (7) for the number of outstanding packets sent by the linkmgr and also enables the operator to configurable a specific number of outstanding packets sent by the linkmgr. These configurations are applicable for both high-speed and low-speed narrowband links.

CLI (Link Configuration Mode)

mtp2-max-outstand-frames <*5 - 10***>**

default mtp2-max-outstand-frames

network-sharing failure-code

Network-sharing reject cause codes can be configured with the following new command:

CLI (IuPS-Service Configuration Mode)

network-sharing failure-code *<2-111>*

default network-sharing failure-code

old-tlli

Part 1: A new command configures a list of random TLLI (identified by hex number) to be invalidated (removed) from the GMM after the invalidate old-TLLI timer expires (see Part 2) and starts the invalidate old-TLLI timer. This command can be repeated up to 50 TLLI.

CLI (SGSN-Global Configuration Mode)

[no] old-tlli invalidate tlli < *hexadecimal* **>**

IMPORTANT

If the old-TLLI expiry timer is not configured with the old-tlli hold-time command, then the SGSN will only drop second Attach Requests using the same random TLLI already in use.

Part 2: Another keyword in this new command configures the old-TLLI expiry timer (1 to 125 seconds, default of 5) to be started in GMM when anyone of the listed random TLLI are received. If the timer expires prior to receiving Attach-Complete then the SGSN invalidates (removes) the TLLI from the GMM.

CLI (SGSN-Global Configuration Mode)

```
[ no ] old-tlli hold-time < seconds >
```

IMPORTANT

For this configuration to work, the list of random TLLI to be removed (invalidated) from the GMM must be defined with the old-tlli invalidate tlli command.

pdp-deactivation-rate

Set the rate at which the SGSN deactivates PDP connections per second per SessMgr when a GPT-C path failure is detected.

CLI (SGSN-Global Configuration Mode)

```
pdp-deactivation-rate { connected-ready <rate> | idle-standby <rate> }
default pdp-deactivation-rate { connected-ready | idle-standby }
```

peer-nri-length

Defining the NRI length (1 - 10) for this new command enables the SGSN to use NRI-FQDN based DNS resolution for non-local RAIs when selection of the call control profile is based on the old-RAI and the PLMN Id of the RNC.

CLI (Call-Control-Profile Configuration Mode)

```
peer-nri-length <length>
remove peer-nri-length
```

IMPORTANT

This configuration is only valid if the call control profile does not have an associated IMSI range.

ptmsi-signature-reallocate

A new command enables configuration of P-TMSI signature reallocation for Attach/RAU procedures.

CLI (SGTP Service Configuration Mode)

```
ptmsi-signature-reallocate { attach | frequency <frequency> | interval
<minutes> | ptmsi-reallocation-command | routing-area-update [ update-type
[ combined-update | imsi-combined-update | periodic | ra-update ] } [
access-type { gprs | umts } ] [ frequency <frequency> ]
```

qos-modification

New CLI command introduced at the SGSN Service Configuration Mode, it provides flexibility to enable/ disable RAB set up followed by UPCQ towards GGSN / Modify towards UE based on whether or not RNC downgrades the QoS. By default, the SGSN informs UE before RNC.

CLI (SGSN Service Configuration Mode)

```
qos-modification inform-rnc-before-ue
no qos-modification
```

rab-asymmetry-indicator

New command enables the SGSN to force “Asymmetric-Bidirectional” as the RAB Asymmetry Indicator when uplink/downlink bitrates are equal.

CLI (RNC Configuration Mode)

```
rab-asymmetry-indicator symmetric-bidirectional
force-asymmetric-bidirectional
no rab-asymmetry-indicator symmetric-bidirectional
force-asymmetric-bidirectional
default rab-asymmetry-indicator
```

ranap excess-len ignore

A new command configures the SGSN to ignore RANAP messages that have extra octets.

CLI (SGSN-Global Configuration Mode)

```
[ default | no ] ranap excess-len ignore
```

ranap global-cn-id

The following new command allows the SGSN to use ‘selected-plmn’ in the Global Core Network ID IE in the Paging Request message and/or the Relocation Request message when network sharing is enabled:

CLI (RNC Configuration Mode)

```
ranap global-cn-id { relocation-request | paging-request } [
network-sharing selected-plmn ]
[ default | no ] ranap global-cn-id { relocation-request | paging-request }
```

ranap paging-area-id

The following new command allows the SGSN to use ‘selected-plmn’ in the Paging Area ID IE in the Paging Request message and/or the Relocation Request message when network sharing is enabled:

CLI (RNC Configuration Mode)

```
ranap paging-area-id paging-request [ network-sharing selected-plmn ]
[ default | no ] ranap paging-area-id paging-request
```

regional-subscription-restriction

This command enables the operator to define the cause code for subscriber rejection when it is due to regional subscription information failure.

CLI (Call-Control Profile Configuration Mode)

```
[ remove ]  regional-subscription-restriction [ failure-code <code> |
user-device-release { before-r99 failure-code <code> | r99-or-later
failure-code <code> } ]
```

relocation-alloc-timeout

A new command defines the amount of time (in seconds) that the SGSN waits for a Relocation Request message. The range is 1 to 60 with a default of 5.

CLI (IuPS Service Configuration Mode)

relocation-alloc-timeout *<time>*

default relocation-alloc-timeout

reporting-action event-record

This new command enables the SGSN to log GMM/SM events in EDR files for SGSN services.

CLI (SGSN-Service Configuration Mode)

[default | no] reporting-action event-record

This new command enables the SGSN to log GMM/SM events in EDR files for 2G services.

CLI (GPRS-Service Configuration Mode)

[default | no] reporting-action event-record

IMPORTANT

To enable CDR file generation, enter the **edr-module active-charging-service**, command from the Context configuration mode. To configure the file transfer and CDR parameters, accesses the EDR module configuration mode commands.

sctp-init-rwnd

A new command enables the SCTP association to set the size of the window (32768 (32KB) to 1048576 (1MB)) at the receiving end. The default window size is 1048576.

IMPORTANT

Before the window size can be set, the ASP association must be terminated with the **no associate** command. After the window size is set, the ASP association must be re-established with the **associate** command.

CLI (SGSN PSP Configuration Mode)

sctp-init-rwnd <*window_size***>**

default sctp-init-rwnd

sgsn retry-unavailable-ggsn

Marks the GGSN as available for further activation.

CLI (Exec Mode)

sgsn retry-unavailable-ggsn *<IPv4 or IPv6>*

smsc-address-restriction-list

A new command allows the operator to restrict forwarding of SMS messages on the basis of a defined list of SMS-C addresses.

CLI (Short-Message-Service Configuration Mode)

smsc-address-restriction-list *<isdn-no>* **+**

no smsc-address-restriction-list *<isdn-no>*

IMPORTANT

The **smsc-address-restriction-list** command only takes effect if the **smsc-address-restriction-type** command has also been configured.

target-offloading algorithm

Configure the number of subscribers to be off-loaded.

CLI (SGSN-Global Configuration Mode)

target-offloading algorithm [optimized-for-speed | optimized-for-target-count]

SGSN Commands - New in Release 12.1

This section provides information on new SGSN commands available in Release 12.1.

access-restriction-data

This new command enables the operator to assign a failure code to be included in reject messages if attach rejection is due to access restriction data (ARD) checking in incoming subscriber data (ISD) messages. As well, the operator can disable the ARD checking behavior.

CLI (Call Control Profile Configuration Mode)

access-restriction-data { failure-code *<cause_code>* **| no-check }**

remove access-restriction-data failure-code

aggregate-ipc-msg

New command enables/disables aggregation of IPC messages in linkmgr and sessmgr.

CLI (SGSN-Global Configuration Mode)

aggregate-ipc-msg { linkmgr | sessmgr } { flush-frequency *<frequency>* **| num-msgs** *<number_msgs>* **}**

default aggregate-ipc-msg { linkmgr | sessmgr }

bssgp-message

A new command determines the SGSN response to MS-Flow-Control messages received from an unknown MS.

CLI (SGSN Global Configuration Mode)

bssgp-message ms-flow-control-from-unknown-ms { discard-message | send-ack | send-status }

[default] bssgp-message ms-flow-control-from-unknown-ms

check-zone-code

Command enables/disables a mechanism to check zone codes.

CLI (Call-Control Profile Configuration Mode)

[no | remove] check-zone-code

ggsn-fail-retry-timer

Sets the amount of time that a GGSN will be unavailable/blacklisted.

CLI (SGTP Service Configuration Mode)

ggsn-fail-retry-timer <*value*>

no ggsn-fail-retry-timer

gn-delay-monitoring

New command enables monitoring of the delay of packets over Gn/Gp between the SGSN and GGSN.

CLI (SGTP Service Configuration Mode)

gn-delay-monitoring [num-delay *<number_delayed>* **| num-no-delay-for-clear <number_normal> | tolerance-seconds** *<number_seconds>* **]**

default gn-delay-monitoring [num-delay | num-no-delay-for-clear | tolerance-seconds]

no gn-delay-monitoring

ignore-remote-restart-counter-change

A new command instructs the SGSN to ignore (not process) restart counters received from remote nodes. Default is to process the restart counters.

CLI (SGTP Service Configuration Mode)

ignore-remote-restart-counter-change

[default | no] ignore-remote-restart-counter-change

mtp2-max-outstand-frames

A new command provides a new default (7) for the number of outstanding packets sent by the linkmgr and also enables the operator to configurable a specific number of outstanding packets sent by the linkmgr. These configurations are applicable for both high-speed and low-speed narrowband links.

CLI (Link Configuration Mode)

mtp2-max-outstand-frames *<5 - 10>*

default mtp2-max-outstand-frames

ptmsi-signature-reallocate

A new command enables configuration of P-TMSI signature reallocation for Attach/RAU procedures.

CLI (SGTP Service Configuration Mode)

ptmsi-signature-reallocate { attach | frequency <frequency> | interval <minutes> | ptmsi-reallocation-command | routing-area-update [update-type [combined-update | imsi-combined-update | periodic | ra-update] } [access-type { gprs | umts }] [frequency *<frequency>* **]**

regional-subscription-restriction

This command enables the operator to define the cause code for subscriber rejection when it is due to regional subscription information failure.

CLI (Call-Control Profile Configuration Mode)

[remove] regional-subscription-restriction [failure-code *<code>* **| user-device-release { before-r99 failure-code** *<code>* **| r99-or-later failure-code** *<code>* **}]**

relocation-alloc-timeout

A new command defines the amount of time (in seconds) that the SGSN waits for a Relocation Request message. The range is 1 to 60 with a default of 5.

CLI (IuPS Service Configuration Mode)

relocation-alloc-timeout *<time>*

default relocation-alloc-timeout

sgsn retry-unavailable-ggsn

Marks the GGSN as available for further activation.

CLI (Exec Mode)

sgsn retry-unavailable-ggsn *<IPv4 or IPv6>*

smsc-address-restriction-list

A new command allows the operator to restrict forwarding of SMS messages on the basis of a defined list of SMS-C addresses.

CLI Short-Message-Service Configuration Mode

smsc-address-restriction-list *<isdn-no>* **+**

no smsc-address-restriction-list *<isdn-no>*

IMPORTANT

The **smsc-address-restriction-list** command only takes effect if the **smsc-address-restriction-type** command has also been configured.

target-offloading algorithm

Configure the number of subscribers to be off-loaded.

CLI (SGSN-Global Configuration Mode)

```
target-offloading algorithm [ optimized-for-speed |
optimized-for-target-count ]
```

SGSN Commands - New in Release 12.2

This section provides information on new SGSN commands available in Release 12.2.

apn-resolve-dns-query snaptr

This new command enables the SGSN to send an straightforward name authority pointer (SNAPTR) type DNS query for APN resolution. The SNAPTR filters based on the EPC-capability of the user equipment (UE).

CLI (SGSN-Global Configuration Mode)

```
[ default | no ] apn-resolve-dns-query snaptr
```

bssgp-message ptp-bvc-reset

This new command enables the operator to specify the action to be taken when the SGSN receives a peer-to-peer BVC-Reset.

CLI (SGSN-Global Configuration Mode)

```
bssgp-message ptp-bvc-reset { frc-subscriber-standby | retain-current-state
}
default bssgp-message ptp-bvc-reset
```

check-imei

New commands determine the SGSN’s action during an attach process if the route towards the EIR is down.

IMPORTANT

The **`check-imei gf-failure-action`** command described below for 2G and 3G SGSNs works only if the EIR is associated under map-service and the EIR link is down. If **`check-imei gf-failure-action`** is configured as **`continue`**, and there is no EIR associated under map-service, then the SGSN rejects the Attach procedure with the disconnect-reason c*heck-imei failure.*

disable-remote-restart-counter-verification

This new command disables the SGSN's default behavior for verification of remote peer's restart counter change values.

CLI (SGTP Service Configuration Mode)

```
[ no | default ] disable-remote-restart-counter-verification
```

dlci-util schema

A new command has been added to the Bulkstats configuration mode to configure bulk statistics collection for the DLCI utilization:

CLI (Bulkstats Configuration Mode)

```
[ no ] dlci-util schema <dlci_schema_name> format <dlci_schema_format>
```

dual-address-pdp

New command makes it possible for the operator to enable (default) / disable SGSN support for MS/UE requests for dual PDP type (IPv4v6) addressing.

NOTE: For this feature to function, **common-flags** must be enabled with the **gptc send** command in the SGTP Service configuration mode.

CLI (SGSN-Global Configuration Mode)

```
[ default | no ] dual-address-pdp
```

dual-address-pdp

This new command enables the SGSN to work with an RNC with functioning dual address (IPv4v6) bearer support capability.

CLI (RNC Configuration Mode)

```
[ default ] dual-address-pdp { not-supported |  supported }
```

empty-cr

This new command allows the operator to enable a feature which determines how empty (no data parameters) Connection Request messages will be handled.

CLI (IuPS Service Configuration Mode)

```
[ default | no ] empty-cr procedure reject
```

force-authenticate consecutive-security-failure

New command disables/enables forced authentication when the MS/UE security fails. Also configures the procedures and frequency for authentication.

CLI (IuPS Service Configuration Mode)

```
force-authenticate consecutive-security-failure { inter-sgsn-rau |
local-messages count <frequency> | non-local-messages count <frequency> }
[ default | no ] force-authenticate consecutive-security-failure {
inter-sgsn-rau | local-messages | non-local-messages }
```

gmm-message

The new command configures the SGSN to discard (drop) the Attach-Request message received with a random TLLI already in use.

CLI (SGSN-Global Configuration Mode)

```
[ default ] gmm-message attach-with-tlli-in-use discard-message
```

map-message

A new configuration command instructs the SGSN to either ignore or validate the CAMEL subscription when there is no CAMEL service associated or in existence.

CLI (SGSN-Global Configuration Mode)

map-message insert-subscriber-data csi-handling when-camel-not-associated ignore-subscription

default map-message insert-subscriber-data csi-handling

max-remote-restart-counter-change

This command sets a restart counter change window to avoid the resulting service deactivations and activations causing large bursts of network traffic if the restart counter change messages from the GGSN are erroneous.

CLI (SGTP Service Configuration Mode)

max-remote-restart-counter-change <*value 1 - 255***>**

default max-remote-restart-counter-change

min-unused-auth-vector

A new configuration command defines a threshold for the minimum number of unused vectors that the SGSN will retain before triggering the initiation of a SAI.

CLI (Call-Control Profile Configuration Mode)

min-unused-auth-vector <*min#_vectors***>**

remove min-unused-auth-vector

network-overload-protection

New **queue-size** and **wait-time** keywords define the queue size for buffering and message age-out wait-time for optimized network overload protection.

CLI (Global Configuration Mode)

network-overload-protection sgsn-new-connections-per-second #_new_connections action { drop | reject with cause { congestion | network failure } } [queue-size *<queue_size>* **] [wait-time** *<wait_time>* **]**

default network-overload-protection

network-sharing failure-code

Network-sharing reject cause codes can be configured with the following new command:

CLI (IuPS-Service Configuration Mode)

network-sharing failure-code *<2-111>*

default network-sharing failure-code

old-tlli

Part 1: A new command configures a list of random TLLI (identified by hex number) to be invalidated (removed) from the GMM after the invalidate old-TLLI timer expires (see Part 2) and starts the invalidate old-TLLI timer. This command can be repeated up to 50 TLLI.

CLI (SGSN-Global Configuration Mode)

```
[ no ] old-tlli invalidate tlli < hexadecimal >
```

IMPORTANT

If the old-TLLI expiry timer is not configured with the old-tlli hold-time command, then the SGSN will only drop second Attach Requests using the same random TLLI already in use.

Part 2: Another keyword in this new command configures the old-TLLI expiry timer (1 to 125 seconds, default of 5) to be started in GMM when anyone of the listed random TLLI are received. If the timer expires prior to receiving Attach-Complete then the SGSN invalidates (removes) the TLLI from the GMM.

CLI (SGSN-Global Configuration Mode)

```
[ no ] old-tlli hold-time < seconds >
```

IMPORTANT

For this configuration to work, the list of random TLLI to be removed (invalidated) from the GMM must be defined with the old-tlli invalidate tlli command.

pdp-deactivation-rate

Set the rate at which the SGSN deactivates PDP connections per second per SessMgr when a GPT-C path failure is detected.

CLI (SGSN-Global Configuration Mode)

```
pdp-deactivation-rate { connected-ready <rate> | idle-standby <rate> }
default pdp-deactivation-rate { connected-ready | idle-standby }
```

pdp-type-ipv4v6-override

This new command configures the SGSN to send either IPv4 or IPv6 towards GGSN when MS/UE requests PDP type as IPv4v6 but either the SGSN or the RNC is not configured to support dual PDP type.

CLI (APN Profile Configuration Mode)

```
pdp-type-ipv4v6-overrride { ipv4 | ipv6 }
remove pdp-type-ipv4v6-overrride
```

ranap excess-len ignore

A new command configures the SGSN to ignore RANAP messages that have extra octets.

CLI (SGSN-Global Configuration Mode)

```
[ default | no ] ranap excess-len ignore
```

ranap global-cn-id

The following new command allows the SGSN to use ‘selected-plmn’ in the Global Core Network ID IE in the Paging Request message and/or the Relocation Request message when network sharing is enabled:

CLI (RNC Configuration Mode)

```
ranap global-cn-id { relocation-request | paging-request } [
network-sharing selected-plmn ]
```

```
[ default | no ] ranap global-cn-id { relocation-request | paging-request }
```

ranap paging-area-id

The following new command allows the SGSN to use ‘selected-plmn’ in the Paging Area ID IE in the Paging Request message and/or the Relocation Request message when network sharing is enabled:

CLI (RNC Configuration Mode)

```
ranap paging-area-id paging-request [ network-sharing selected-plmn ]
```

```
[ default | no ] ranap paging-area-id paging-request
```

ran-information-management

This new command enables the SGSN to handle RIM messages if the destination node is also RIM capable.

CLI (SGSN Global Configuration Mode)

```
[ default | no ] ran-information-management
```

ran-information-management

This new command informs the SGSN that the RNC is RIM capable.

NOTE: to use this command, RIM support must first be enabled in the SGSN Global configuration mode.

CLI (RNC Configuration Mode)

```
[ default | no ] ran-information-management
```

reporting-action event-record

This new command enables the SGSN to log GMM/SM events in EDR files for SGSN services.

CLI (SGSN-Service Configuration Mode)

```
[ default | no ] reporting-action event-record
```

This new command enables the SGSN to log GMM/SM events in EDR files for 2G services.

CLI (GPRS-Service Configuration Mode)

[default | no] reporting-action event-record

IMPORTANT

To enable CDR file generation, enter the **edr-module active-charging-service**, command from the Context configuration mode. To configure the file transfer and CDR parameters, accesses the EDR module configuration mode commands.

sctp-init-rwnd

A new command enables the SCTP association to set the size of the window (32768 (32KB) to 1048576 (1MB)) at the receiving end. The default window size is 1048576.

IMPORTANT

Before the window size can be set, the ASP association must be terminated with the **no associate** command. After the window size is set, the ASP association must be re-established with the **associate** command.

CLI (SGSN PSP Configuration Mode)

sctp-init-rwnd <*window_size*>

default sctp-init-rwnd

TPO Commands - New in Release 12.0

This section provides information on new TPO commands available in Release 12.0.

p2p-detected

This command allows to disable/continue TPO optimizations when a P2P flow is detected.

CLI (ACS TPO Profile Configuration Mode)

p2p-detected { cease-tpo | continue-tpo }

default p2p-detected

tpo default-policy

This command configures the default TPO policy for a rulebase. For subscribers using a particular rulebase, the default TPO policy configured in it will be used only if in the APN/subscriber profile no TPO policy is configured, and a policy to use is not received from the AAA.

CLI (ACS Rulebase Configuration Mode)

tpo default-policy *tpo_policy_name*

no tpo default-policy

tpo profile

This command configures the TPO profile for the charging action. This enables the specified TPO profile to be applied when a flow matches the charging action.

CLI (ACS Charging Action Configuration Mode)

tpo profile *tpo_profile_name*

no tpo profile

TPO Commands - New in Release 12.2

This section provides information on new TPO commands available in Release 12.2.

tcp pacing

This command enables/disables TCP Pacing support, which causes the sender to evenly distribute window of data over an entire RTT.

CLI (ACS TPO Profile Configuration Mode)

[no | default] tcp pacing

Modified Configuration Commands

This section identifies configuration commands that have been modified in Release 12.x.

Common Commands - Modified in Release 12.0

This section provides information on common commands modified for Release 12.0.

authentication

This command configures authentication for subscribers or gateways accessing a service using the crypto template. Two new keywords and their respective supporting keywords and variables were added to the **authentication** command in the Crypto Template Configuration Mode: **local** and **remote**.

CLI (Crypto Template Configuration Mode)

authentication { eap-profile *name* **[second-phase eap-profile** *name* **] | gateway { encrypted key** *value* **| key** *clear_text* **} | local { certificate | pre-shared-key { encrypted key** *value* **| key** *clear_text* **} | pre-shared-key { encrypted key** *value* **| key** *clear_text* **} | remote { certificate | eap-profile** *name* **[second-phase eap-profile** *name* **] | pre-shared-key { encrypted key** *value* **| key** *clear_text* **} }**

clock

The new **asia-almaty** option for the **timezone** keyword allows the operator to configure the system clock's timezone for Almaty, Kazakhstan.

CLI (Global Configuration Mode)

clock timezone asia-almaty

diameter dictionary

This command configures the Diameter Credit Control dictionary for the Active Charging Service. In this release, the **dcca-custom21** through **dcca-custom30** options were added to this command.

CLI (Credit Control Configuration Mode)

diameter dictionary { dcca-custom1 | dcca-custom10 | dcca-custom11 | dcca-custom12 | dcca-custom13 | dcca-custom14 | dcca-custom15 | dcca-custom16 | dcca-custom17 | dcca-custom18 | dcca-custom19 | dcca-custom2 | dcca-custom20 | dcca-custom21 | dcca-custom22 | dcca-custom23 | dcca-custom24 | dcca-custom25 | dcca-custom26 | dcca-custom27 | dcca-custom28 | dcca-custom29 | dcca-custom3 | dcca-custom30 | dcca-custom4 | dcca-custom5 | dcca-custom6 | dcca-custom7 | dcca-custom8 | dcca-custom9 | standard }

default diameter dictionary

ikev2-ikesa

The **allow-empty-ikesa** keyword is new in the **ikev2-ikesa** command allowing the retention of an IKE SA even after its child SAs have been deleted.

CLI (Crypto Template Configuration Mode)

ikev2-ikesa { allow-empty-ikesa | keepalive-user-activity | max-retransmissions *number* **| retransmission-timeout** *msec* **| policy**

error-notification [invalid-message-id | invalid-syntax] rekey | setup-timer *sec* **| transform-set list** *name* **}**

ip address

This command now allows the configuration of a 31-bit subnet mask for IPv4 addresses per RFC 3021.

CLI (Ethernet Interface Configuration Mode)

ip address *ip_address ip_mask*

link-aggregation

This command is used to aggregate ports on a Quad Gig-E line card (QGLC) and set related parameters. Several keywords have been added.

CLI (Ethernet Port Configuration Mode)

link-aggregation { distribution { block | random | rotate | simple } | lacp { active | passive } [rate { auto | fast | slow }] [timeout { long | short }] | master { global group *group_number* **| group** *group_number* **| local group** *group_number* **} | member { global group** *group_number* **| group** *group_number* **| local group** *group_number* **} | redundancy { standard | switched } [hold-time** *sec* **] [preferred slot {** *card_number* **| none }] | toggle-link }**

no link-aggregation [toggle-link]

default link-aggregation { distribution | lacp | redundancy | toggle-link }

For **link-aggregation redundancy standard** mode, **hold-time** and **preferred slot** settings are now accepted and processed. Previously these settings were only observed for **link-aggregation redundancy switched** mode.

match ip pool

The keyword **destination-network** has been added to this command. An IP pool attached to the crypto map can have multiple IPSec tunnels according to the destination of the packet being forwarded to internet.

CLI (Crypto Map IKEv1 Configuration Mode)

[no] match ip pool pool-name *pool_name* **[destination-network** *ip_address* **{ /** *mask* **| mask** *ip_mask* **}]**

pending-traffic-treatment

This command controls the pass/drop treatment of traffic while waiting for definitive credit information from the server. In this release, a new keyword **limted-pass** has been added to this command. This enables limited access for subscribers when the OCS is unreachable by provisioning a default quota to use until there is a response from the OCS.

CLI (Credit Control Configuration Mode)

pending-traffic-treatment { { { forced-reauth | trigger | validity-expired } drop | pass } | { { noquota | quota-exhausted } buffer | drop | limited-pass *volume* **| pass } }**

default pending-traffic-treatment { forced-reauth | noquota | quota-exhausted | trigger | validity-expired }

radius attribute

This command configures the system's RADIUS identification parameters. The keyword **accounting** has been added to enable/disable RADIUS accounting attributes for the following options, provided they are supported in the configured RADIUS dictionary:

- 3GPP-CG-Address
- 3GPP-Chrg-Char
- 3GPP-Charging-ID
- 3GPP-GGSN-Address
- 3GPP-GGSN-Mcc-Mnc
- 3GPP-GPRS-QoS-Negotiated-Profile
- 3GPP-IMEISV
- 3GPP-IMSI-Mcc-Mnc
- 3GPP-MS-TimeZone
- 3GPP-NSAPI
- 3GPP-PDP-Type
- 3GPP-RAT-Type
- 3GPP-Selection-Mode
- 3GPP-SGSN-Address
- 3GPP-SGSN-Mcc-Mnc
- 3GPP-User-Location-Info
- Acct-Input-Octets
- Acct-Input-Packets
- Acct-Output-Octets
- Acct-Output-Packets
- Acct-Session-Time
- Called-Station-ID
- Calling-Station-ID
- Event-Timestamp
- IMSI

The keyword **authentication** has been added to enable/disable RADIUS authentication attributes for the following options, provided they are supported in the configured RADIUS dictionary:

- 3GPP-CG-Address
- 3GPP-Chrg-Char

- 3GPP-GGSN-Address
- 3GPP-GGSN-Mcc-Mnc
- 3GPP-GPRS-QoS-Negotiated-Profile
- 3GPP-IMEISV
- 3GPP-IMSI-Mcc-Mnc
- 3GPP-MS-TimeZone
- 3GPP-NSAPI
- 3GPP-PDP-Type
- 3GPP-RAT-Type
- 3GPP-Selection-Mode
- 3GPP-SGSN-Address
- 3GPP-SGSN-Mcc-Mnc
- 3GPP-User-Location-Info
- Called-Station-ID
- Calling-Station-ID
- IMSI

CLI (AAA Server Group Configuration Mode)

radius attribute { accounting *accounting_attribute* | **authentication** *authentication_attribute* | **nas-identifier** *nas_id* | **nas-ip-address address** *primary_address* **[backup** *secondary_address* **] [nexthop-forwarding-address** *nexthop_address* **] [mpls-label input** *in_label_value* | **output** *out_label_value1* **[** *out_label_value2* **] [** *vlan vlan_id* **]] }**

no radius attribute { accounting *accounting_attribute* | **authentication** *authentication_attribute* | **nas-identifier** | **nas-ip-address }**

default radius attribute { accounting | **authentication** | **nas-identifier }**

rule-variable

This command specifies the order of fields in the EDR. The following new TPO-related fields are now supported in the EDR format:

- TCP flow related:
  - tpo-enabled
- HTTP transaction related:
  - ad-delivered
  - ad-replaced
  - compression-bytes-in
  - compression-bytes-out
  - dns-resolution-locally
  - dns-resolution-remotely
  - tpo-enabled

CLI (ACS EDR Format Configuration Mode)

rule-variable *protocol rule* **priority** *priority* **[in-quotes]**

no rule-variable *protocol rule* **[priority** *priority* **]**

use-proxy

This command enables a Diameter proxy for the Diameter endpoint. A new keyword **server-mode** is added in this release to specify that the Diameter proxy should be treated as if it is the server side of the endpoint connection.

CLI (Diameter Endpoint Configuration Mode)

use-proxy [server-mode [demux-mode]]

Common Commands - Modified in Release 12.2

This section provides information on common commands modified for Release 12.2.

aaa constructed-nai

Configures the password used during authentication for sessions using a Constructed Network Access Identifier (NAI) or an APN-specified user name. The maximum value for the keyword **encrypted password** has been changed from 63 to 132 characters.

CLI (Context Configuration Mode)

aaa constructed-nai authentication [[encrypted] password *user_password* **| useshared-secret-password]**

no aaa constructed-nai authentication

cc

This command configures a charging characteristics profile, within the accounting profile configuration, for CDR generation. In this release, the maximum value for the cc profile buckets has been extended to support up to 10 for Diameter Rf accounting only. However, in the case of GTPP accounting, this CLI command allows configuring only up to 4 buckets.

Also, the maximum limit for the volume octets has been changed from 400000000 to 4000000000.

CLI (Accounting Policy Configuration Mode)

cc profile *index* **{ buckets** *num* **| interval** *seconds* **| sdf-interval** *seconds* **| sdf-volume { downlink** *octets* **{ uplink** *octets* **} | total** *octets* **| uplink** *octets* **{ downlink** *octets* **} } | serving-nodes** *num* **| tariff time1** *min hrs* **[time2** *min hrs***...time4** *min hrs* **] | volume { downlink** *octets* **{ uplink** *octets* **} | total** *octets* **| uplink** *octets* **{ downlink** *octets* **} } }**

default cc profile *index*

no cc profile *index* **{ buckets | interval | sdf-interval | sdf-volume | serving-nodes | tariff | volume }**

cca radius user-password

Specifies the RADIUS prepaid service subscriber's user password parameters in the rulebase. The maximum value for the keyword **encrypted password** has been changed from 63 to 132 characters.

CLI (ACS Rulebase Configuration Mode)

cca radius user-password [encrypted] password *password*

[no] cca radius user-password

diameter peer-select

This command configures the Diameter credit control primary and secondary hosts for DCCA. A new keyword **msisdn-based** has been added to this command to support Diameter peer selection based on MSISDN prefix/suffix/range.

CLI (Credit Control Configuration Mode)

diameter peer-select peer *peer_name* **[realm** *realm_name* **] [secondary-peer** *secondary_peer_name* **[realm** *realm_name* **]] [imsi-based { { prefix | suffix }** *imsi/prefix/suffix_start_value* **} [to** *imsi/prefix/suffix_end_value* **]] [msisdn-based { { prefix | suffix }** *msisdn-based/prefix/suffix_start_value* **} [to** *msisdn-based/prefix/suffix_end_value* **]]**

no diameter peer-select [imsi-based { { prefix | suffix } *imsi/prefix/suffix_start_value* **} [to** *imsi/prefix/suffix_end_value* **]] | [msisdn-based { { prefix | suffix }** *msisdn-based/prefix/suffix_start_value* **} [to** *msisdn-based/prefix/suffix_end_value* **]]**

diameter result-code

This command enables sending GTP Create-PDP-Context-Rsp message with cause code based on the DCCA result code. The following keywords were newly added to this command:

- **credit-limit-reached**
- **end-user-service-denied**
- **system-failure**

CLI (Credit Control Configuration Mode)

diameter result-code { authorization-rejected | credit-limit-reached | end-user-service-denied | user-unknown } use-gtp-cause-code { authentication-failure | no-resource-available | system-failure }

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

flow action redirect-url

The following allowed dynamic fields have been added to this command:

- #CONTENT-ID-LABEL#
- #CONTENT-ID-LABEL-CAUSING-REDIRECTION#
- #BEARER.HWID#
- #BEARER.IMSI#
- #BEARER.IMEI#
- #BEARER.ESN#
- #BEARER.MEID#

Concatenated dynamic fields separated by ";" can also be added (for example, #BEARER.IMEI;BEARER.IMSI#).

In addition, the keywords **encryption { blowfish128 | blowfish64 } [encrypted] key** *key* enable encryption for dynamic fields of redirect url.

CLI (ACS Charging Action Configuration Mode)

flow action redirect-url *url* **/%3furl=** *dynamic_field*
[clear-quota-retry-timer] [encryption { blowfish128 | blowfish64 }
[encrypted] key *key* **]**

no flow action

gtpc

The following keyword has been added to this command:

- **path-failure detection-policy echo**

CLI (eGTP Service Configuration Mode)

gtpc { bind { ipv4-address *ipv4_address* **[ipv6-address** *ipv6_address* **] | ipv6-address** *ipv6_address* **[ipv4-address** *ipv4_address* **] } | echo-interval** *seconds* **| ip qos-dscp {** *forwarding_type* **} | max-retransmissions** *num* **| path-failure detection-policy echo | retransmission-timeout** *seconds* **}**

no gtpc { bind { ipv4-address *ipv4_address* **[ipv6-address** *ipv6_address* **] | ipv6-address** *ipv6_address* **[ipv4-address** *ipv4_address* **] } | echo-interval | path-failure detection-policy }**

default gtpc { echo-interval | ip qos-dscp | max-retransmissions | path-failure detection-policy | retransmission-timeout }

gtpp dictionary

The following new gtpp dictionaries have been added to this command:

custom41, custom42, custom43, custom44, custom45, custom46, custom47, custom48, custom49, custom50, custom51, custom52, custom53, custom54, custom55, custom56, custom57, custom58, custom59, and custom60

CLI (Context Configuration Mode)

gtpp dictionary { **custom1 | custom10 | custom11 | custom12 | custom13 | custom14 | custom15 | custom16 | custom17 | custom18 | custom19 | custom2 | custom20 | custom21 | custom22 | custom23 | custom24 | custom25 | custom26 | custom27 | custom28 | custom29 | custom3 | custom30 | custom31 | custom32 | custom33 | custom34 | custom35 | custom36 | custom37 | custom38 | custom39 | custom4 | custom40 | custom41 | custom42 | custom43 | custom44 | custom45 | custom46 | custom47 | custom48 | custom49 | custom5 | custom50 | custom51 | custom52 | custom53 | custom54 | custom55 | custom56 | custom57 | custom58 | custom59 | custom6 | custom60 | custom7 | custom8 | custom9 | standard** }

gtpp trigger

This command disables or enables GTPP trigger conditions that cause either partial CDR record closure or opening of a new CDR record container. In this release, this command has been enhanced to accept the following new keywords:

- **generate { cdr | container } –** for choice of generation of CDR or just a container on a RAT change
- **uli-change** – for enabling the user location update trigger for eG-CDRs/PGW-CDRs, if the dictionary specified in the GTPP dictionary configuration includes support for user location update trigger

CLI (GTPP Server Group Configuration Mode)

gtpp trigger { cell-update | direct-tunnel | egcdr max-losdv | ggsn-preservation-mode-change | inter-plmn-sgsn-change | ms-timezone-change | plmn-id-change | qos-change | rat-change [generate { cdr | container }] | routing-area-update | sgsn-change-limit | serving-node-change-limit | tariff-time-change | time-limit | uli-change | volume-limit }

default gtpp trigger

no gtpp trigger { cell-update | direct-tunnel | egcdr max-losdv | ggsn-preservation-mode-change | inter-plmn-sgsn-change | ms-timezone-change | plmn-id-change | qos-change | rat-change | routing-area-update | sgsn-change-limit | serving-node-change-limit | tariff-time-change | time-limit | uli-change | volume-limit }

radius accounting server

This command configures the RADIUS accounting server(s) in the current context. The maximum value for the keyword **encrypted key** has been changed from 256 to 236 characters.

CLI (AAA Server Group Configuration Mode and Context Configuration Mode)

radius [mediation-device] accounting server *ip_address* **[encrypted] key** *value* **[acct-on { disable | enable }] [acct-off { disable | enable }] [adminstatus { disable | enable }] [max** *max_messages* **] [max-rate** *max_value* **] [oldports] [port** *port_number* **] [priority** *priority* **] [type { mediation-device | standard }] [-noconfirm]**

no radius [mediation-device] accounting server *ip_address* **[oldports | port** *port_number* **]**

radius charging accounting server

Configures RADIUS charging accounting servers in the current context for Active Charging Service Prepaid Accounting. The maximum value for the keyword **encrypted key** has been changed from 256 to 236 characters.

CLI (AAA Server Group Configuration Mode and Context Configuration Mode)

radius charging accounting server *ip_address* **[encrypted] key** *key* **[max** *max_messages* **] [max-rate** *max_rate* **] [oldports] [port** *port_number* **] [priority** *priority* **] [admin-status { enable | disable }] [-noconfirm]**

no radius charging accounting server *ip_address* **[oldports | port** *port_number* **]**

radius change-authorize-nas-ip

Configures the NAS IP address and UDP port on which the current context will listen for Change of Authorization

(COA) messages and Disconnect Messages (DM). If the NAS IP address is not defined with this command, any COA or DM messages from the RADIUS server are returned with a Destination Unreachable error. The maximum value of the keyword **encrypted key** has been changed from 256 to 236 characters.

CLI (Context Configuration Mode)

[no] radius change-authorize-nas-ip *ip_address* **[encrypted] key** *value* **[port** *port* **] [event-timestamp-window** *window* **] [no-nas-identification-check] [no-reverse-path-forward-check] [mpls-label input** *in_label_value* **| output** *out_label_value1* **[** *out_label_value2* **]**

radius charging server

Configures the RADIUS charging server(s) in the current context for Active Charging Service Prepaid Authentication. The maximum value for the keyword **encrypted key** has been changed from 256 to 236 characters.

CLI (AAA Server Group Configuration Mode and Context Configuration Mode)

radius charging server *ip_address* **[encrypted] key** *key* **[max** *max_messages* **] [max-rate** *max_rate* **] [oldports] [port** *port_number* **] [priority** *priority* **] [admin-status { enable | disable }] [-noconfirm]**

no radius charging server *ip_address* **[oldports | port** *port_number* **]**

radius server

This command configures RADIUS authentication server(s) in the current context for authentication. The maximum value for the keyword **encrypted key** has been changed from 256 to 236 characters.

CLI (AAA Server Group Configuration Mode and Context Configuration Mode)

radius server *ip_address* **[encrypted] key** *value* **[admin-status { disable | enable }] [max** *max_messages* **] [max-rate** *max_value* **] [oldports] [port** *port_number* **] [priority** *priority* **] [probe | no-probe] [probe-username** *user_name* **] [probe-password [encrypted] password** *password* **] [type { mediation-device | standard }] [-noconfirm]**

no radius server *ip_address* **[oldports | port** *port_number* **]**

servers-unreachable

This command configures whether to continue/terminate calls when Diameter server(s)/OCS become unreachable. In this release, this command has been enhanced to accept the following additional keywords **after-inter-time**, **after-inter-volume**, and **server-retries**. This CLI command can also be used to control the triggering of behavior either at transport failure, response timeout or at Tx expiry when OCS becomes unreachable.

CLI (Credit Control Configuration Mode)

servers-unreachable { behavior-triggers { initial-request | update-request } transport-failure [response-timeout | tx-expiry] | initial-request { continue [{ [after-interim-time *timeout_period* **] [after-interim-volume** *quota_value* **] } server-retries** *retry_count* **] | terminate [{ [after-interim-time** *timeout_period* **] [after-interim-volume** *quota_value* **] } server-retries** *retry_count* **| after-timer-expiry** *timeout_period* **] } |**

update-request { continue [{ [after-interim-time *timeout_period* **] [after-interim-volume** *quota_value* **] } server-retries** *retry_count* **] | terminate [{ [after-interim-time** *timeout_period* **] [after-interim-volume** *quota_value* **] } server-retries** *retry_count* **] | after-quota-expiry | after-timer-expiry** *timeout_period* **] } }**

no servers-unreachable { initial-request | update-request }

default servers-unreachable behavior-triggers { initial-request | update-request }

save configuration

The new **obsolete-encryption** keyword for the **save configuration** command allows the user to save a pre-12.2 release configuration prior to upgrading to 12.2 A change in encryption method prevents downgrading to a pre-12.2 release and importing a configuration file that had not been saved using this keyword.

CLI (Exec Mode)

save configuration *<url>* **[-redundant] [-noconfirm] [obsolete-encryption] [showsecrets] [verbose]**

system

This new keyword allows the administrator to configure the system description and the system OID string to display both either in the default style or the new Cisco style.

The description only applies to the default description when the admin has not configured the description using the system description CLI.

The OID string is either the current default string 1.3.6.1.4.1.8164 or the new Cisco string 1.3.6.1.4.1.9.

IMPORTANT

This CLI only works on both terms in the keyword. Either both are “default,” or both are “new.”

CLI (Global Config Mode)

sysdesc-sysoid-style new|default

trigger type

This command enables or disables triggering a credit reauthorization when the named values in the subscriber session changes. In this release, the **mcc** and **mnc** keywords were added to this command.

CLI (Credit Control Configuration Mode)

[no] trigger type { cellid | lac | | mcc | mnc | qos | rat | serving-node | sgsn } +

default trigger type

Application Detection and Control - Modified in Release 12.0

This section provides information on ADC commands modified in Release 12.0.

p2p-detection protocol

This command enables detection of peer-to-peer (P2P) protocols. The following keywords were added to this command:

- **blackberry**
- **gmail**
- **itunes**
- **myspace**
- **teamviewer**
- **twitter**
- **viber**

CLI (ACS Configuration Mode)

[no] p2p-detection protocol [actsync | aimini | all | applejuice | ares | armagettron | battlefld | bittorrent | blackberry | citrix | clubpenguin | crossfire | ddlink | directconnect | dofus | edonkey | facebook | facetime | fasttrack | feidian | fiesta | filetopia | florensia | freenet | fring | funshion | gadugadu | gamekit | gnutella | gmail | gtalk | guildwars | halflife2 | hamachivpn | iax | icecast | imesh | iptv | irc | isakmp | iskoot | itunes | jabber | kontiki | manolito | maplestory | meebo | mgcp | msn | mute | myspace | nimbuzz | octoshape | off | oovoo | openft | orb | oscar | paltalk | pando | pandora | popo | pplive | ppstream | ps3 | qq | qqgame | qqlive | quake | rdp | rfactor | rmstream | secondlife | shoutcast | skinny | skype | slingbox | sopcast | soulseek | splashfighter | ssdp | stealthnet | steam | stun | teamspeak | teamviewer | thunder | tor | truphone | tvants | tvuplayer | twitter | uusee | veohtv | viber | vpnx | vtun | warcft3 | wii | winmx | winny | wmstream | wofkungfu | wofwarcraft | xbox | xdcc | yahoo | yourfreetunnel | zattoo +]

p2p protocol

This command enables detection of specific P2P protocols for charging purposes. This release now supports the following protocols:

- Blackberry
- Gmail
- iTunes
- MySpace
- TeamViewer
- Twitter
- Viber

CLI (ACS Ruledef Configuration Mode)

[no] p2p protocol *operator protocol*

p2p traffic-type

This command defines rule expressions to match traffic type—audio, video, and unclassified. The following options were added to this command:

- audio
- video
- unclassified

CLI (ACS Ruledef Configuration Mode)

[no] p2p traffic-type *operator traffic_type*

Application Detection and Control - Modified in Release 12.2

This section provides information on ADC commands modified in Release 12.2.

p2p-detection protocol

This command enables detection of peer-to-peer (P2P) protocols. The following keywords were added to this command:

- **antsp2p**
- **imo**
- **mypeople**
- **netmotion**
- **ogg**
- **openvpn**
- **quicktime**
- **rdt**
- **scydo**
- **spotify**
- **tango**
- **tunnelvoice**
- **ultrabac**
- **usenet**
- **whatsapp**

CLI (ACS Configuration Mode)

[no] p2p-detection protocol [actsync | aimini | all | antsp2p | applejuice | ares | armagettron | battlefld | bittorrent | blackberry | citrix | clubpenguin | crossfire | ddlink | directconnect | dofus | edonkey | facebook | facetime | fasttrack | feidian | fiesta | filetopia | florensia | freenet | fring | funshion | gadugadu | gamekit | gnutella | gmail | gtalk | guildwars | halflife2 | hamachivpn | iax | icecast | imesh | imo | iptv | irc | isakmp | iskoot | itunes | jabber | kontiki | manolito | maplestory | meebo | mgcp | msn | mute | mypeople | myspace | netmotion | nimbuzz | octoshape | off | ogg | oovoo | openft | openvpn | orb | oscar | paltalk | pando | pandora | popo | pplive | ppstream | ps3 | qq | qqgame | qqlive | quake | quicktime | rdp | rdt | rfactor | rmstream | scydo | secondlife | shoutcast | skinny | skype | slingbox | sopcast | soulseek | splashfighter | spotify | ssdp | stealthnet | steam | stun | tango | teamspeak | teamviewer | thunder | tor | truphone | tunnelvoice | tvants | tvuplayer | twitter | ultrabac | usenet | uusee | veohtv | viber | vpnx |

vtun | warcft3 | whatsapp | wii | winmx | winny | wmstream | wofkungfu | wofwarcraft | xbox | xdcc | yahoo | yourfreetunnel | zattoo +]

p2p protocol

This command enables detection of specific P2P protocols for charging purposes. This release now supports the following protocols:

- AntsP2P
- IMO
- MyPeople
- Netmotion
- OGG
- OpenVPN
- Quicktime
- RDT
- Scydo
- Spotify
- Tango
- TunnelVoice
- Ultrabac
- Usenet
- WhatsApp

CLI (ACS Ruledef Configuration Mode)

[no] p2p protocol *operator protocol*

Content Filtering Commands - Modified in Release 12.0

This section provides information on Content Filtering commands modified in Release 12.0.

analyze

This command specifies the action to take for the indicated result after content filtering analysis. The following options are additionally supported for the *category* keyword:

- BACKUP
- CDN
- PHOTO
- PLAG

CLI (Content Filtering Policy Configuration Mode)

analyze priority *priority* **{ all | category** *category* **| x-category** *string* **}**
action { allow | content-insert *content_string* **| discard | redirect-url** *url* **|**
terminate-flow | www-reply-code-and-terminate-flow *reply_code* **} [edr**
edr_format_name **]**

Content Filtering Commands - Modified in Release 12.2

This section provides information on Content Filtering commands modified in Release 12.2.

analyze

This command specifies the action to take for the indicated result after content filtering analysis. The **edr** keyword has been deprecated and replaced with the **reporting-edr** keyword.

CLI (ACS Content Filtering Policy Configuration Mode)

analyze priority *priority* **{ all** | **category** *category* | **x-category** *string* **}** **action { allow** | **content-insert** *content_string* | **discard** | **redirect-url** *url* | **terminate-flow** | **www-reply-code-and-terminate-flow** *reply_code* **} [** **reporting-edr** *reporting_edr_format_name* **]**

no analyze priority *priority*

ECS Commands - Modified in Release 12.0

This section provides information on ECS commands modified in Release 12.0.

group-of-ruledefs-application

This command specifies the purpose of setting up a group-of-ruledefs. In support for the GX Alias feature the **gx-alias** keyword was added to this command. This enables to specify that a group-of-ruledefs is for Gx-alias purposes.

CLI (ACS Group-of-Ruledefs Configuration Mode)

group-of-ruledefs-application { charging | **content-filtering** | **gx-alias** | **post-processing }**

no group-of-ruledefs-application

insert

This command configures the x-header fields to be inserted in HTTP/WSP GET and POST request packets. The **qos** and **s-mcc-mnc** keywords were added to this command. This enables inserting bearer QoS and serving node MCC + MNC in x-headers.

CLI (ACS x-header Format Configuration Mode)

insert *xheader_field_name* **{ string-constant** *xheader_field_value* | **variable { bearer { 3gpp { apn** | **charging-characteristics** | **charging-id** | **imei** | **imsi** | **qos** | **rat-type** | **s-mcc-mnc** | **sgsn-address } | acr** | **customer-id** | **ggsn-address** | **mdn** | **radius-calling-station-id** | **session-id** | **sn-rulebase** | **subscriber-ip-address** | **username } [encrypt]** | **http { host** | **url } }**

no insert *xheader_field_name*

pop3 reply args

This command defines rule expressions to match specified arguments with POP3 reply. In this release, the user-specified argument must be 1 through 127 characters in length. In 11.0

and earlier releases, argument must be an alpha and/or numeric string of 1 through 512 characters in length.

CLI (ACS Ruledef Configuration Mode)

[no] pop3 reply args [case-sensitive] *operator argument*

rule-variable

This command configures the order of fields in the EDR. This command now enables to configure HTTP domain and WSP domain fields in the EDR. For this, from the URL, after http:// (if it is present) is removed, everything until the first "/" is used as the domain.

CLI (ACS Ruledef Configuration Mode)

rule-variable *protocol rule* **priority** *priority* **[in-quotes]**

no rule-variable *protocol rule* **[priority** *priority* **]**

ECS Commands - Modified in Release 12.2

This section provides information on ECS commands modified in Release 12.2.

attribute

This command specifies the order of fields in EDRs. Support for the following new attribute was added to this command.

sn-charge-volume: The total charge volume excluding packets/bytes dropped/retransmitted by ECS.

CLI (EDR Format Configuration Mode)

attribute *attribute* **{ [format { MM/DD/YY-HH:MM:SS | MM/DD/YYYY-HH:MM:SS | YYYY/MM/DD-HH:MM:SS | YYYYMMDDHHMMSS | seconds }] [localtime] | [{ ip | tcp } { bytes | pkts } { downlink | uplink }] priority** *priority* **}**

no attribute *attribute* **[priority** *priority* **]**

billing-action

This command configures billing actions for packets that match ruledefs. Support for configuring charging and reporting EDR formats was added to this command.

CLI (ACS Charging Action Configuration Mode)

billing-action { create-edrs { charging-edr *charging_edr_format_name* **| reporting-edr** *reporting_edr_format_name* **} + [wait-until-flow-ends] | egcdr | exclude-from-udrs | radius | rf } +**

no billing-action [create-edrs | egcdr | exclude-from-udrs | radius | rf] +

cdr

This command configures the EDR/UDR file parameters. The **module-only** keyword was added to this command. This keyword specifies that the transfer-mode is only applicable to

the EDR module; if not configured it is applicable to both EDR and UDR modules. This enables to support individual record transfer-mode configuration for each module.

CLI (EDR Module Configuration Mode)

cdr [[push-interval *value* **] [push-trigger space-usage-percent** *trigger_percentage* **] [remove-file-after-transfer] [transfer-mode { pull | push primary { encrypted-url** *encrypted_url* **| url** *url* **} [via local-context] [secondary { encrypted-secondary-url** *encrypted_secondary_url* **| url** *secondary_url* **}] [module-only] }] + | use-harddisk]**

no cdr [remove-file-after-transfer | use harddisk] +

default cdr [push-interval | push-trigger space-usage-percent | remove-file-after-transfer | transfer-mode [push via] | use harddisk] +

cdr

This command configures the EDR/UDR file parameters. The **module-only** keyword was added to this command. This keyword specifies that the transfer-mode is only applicable to the UDR module; if not configured it is applicable to both EDR and UDR modules. This enables to support individual record transfer-mode configuration for each module.

CLI (UDR Module Configuration Mode)

cdr [push-interval *value* **] [push-trigger space-usage-percent** *trigger_percentage* **] [remove-file-after-transfer] [transfer-mode { pull | push primary { encrypted-url** *encrypted_url* **| url** *url* **} [via local-context] [secondary { encrypted-secondary-url** *encrypted_secondary_url* **| url** *secondary_url* **}] [module-only] }] + | use-harddisk]**

no cdr [remove-file-after-transfer | use-harddisk] +

default cdr [push-interval | push-trigger space-usage-percent | remove-file-after-transfer | transfer-mode [push via] | use-harddisk] +

edr-module active-charging-service

This command enables to create/configure/delete the Event Data Record (EDR) module for the context. Support for configuring the EDR module for charging / reporting EDRs was added to this command.

CLI (Context Configuration Mode)

[no] edr-module active-charging-service [charging | reporting]

edr transaction-complete

This command configures the generation of an EDR on the completion of a transaction. Support for configuring charging and reporting EDR formats was added to this command. The **edr-format** option is supported only in 12.1 and earlier releases. In 12.2 and later releases, it is deprecated and replaced by the **charging-edr** option.

CLI (ACS Rulebase Configuration Mode)

edr transaction-complete http [charging-edr *charging_edr_format_name* **|** **edr-format** *edr_format_name* **|** **reporting-edr** *reporting_edr_format_name* **]**

{ default | no } edr transaction-complete

edr voip-call-end

This command enables generating Event Data Record (EDR) on the completion of voice calls. Support for configuring charging and reporting EDR formats was added to this command. The **edr-format** option is supported only in 12.1 and earlier releases. In 12.2 and later releases, it is deprecated and replaced by the **charging-edr** option.

CLI (ACS Rulebase Configuration Mode)

edr voip-call-end { charging-edr *charging_edr_format_name* **|** **edr-format** *edr_format_name* **|** **reporting-edr** *reporting_edr_format_name* **}+**

{ default | no } edr voip-call-end

flow action

This command specifies the actions for packets that match a rule definition. This command also specifies action on packet and flow for Session Control functionality. Support for Blowfish encryption in conjunction with URL redirection was added to this command.

CLI (ACS Charging Action Configuration Mode)

flow action { conditional user-agent end-token *end_token_name* **|** **discard [downlink | uplink] | random-drop interval** *interval_start* **to** *interval_end* **pkts-to-drop** *packet_min* **to** *packet_max* **| readdress [server** *ipv4_address* **] [port** *port_number* **] | redirect-url** *redirect_url* **[[encryption { blowfish128 | blowfish64 } [encrypted] key** *key* **] clear-quota-retry-timer] | terminate-flow | terminate-session }**

no flow action

flow end-condition

This command sets the end condition of the session flows related to a user session and triggers EDR generation. Support for configuring charging and reporting EDR formats was added to this command.

CLI (ACS Rulebase Configuration Mode)

flow end-condition { content-filtering | hagr | handoff | normal-end-signaling | session-end | url-blacklisting | timeout } [flow-overflow] + { charging-edr *charging_edr_format_name* **|** **reporting-edr** *reporting_edr_format_name* **}**

no flow end-condition

group-of-ruledefs-application

This command specifies the purpose of setting up a group-of-ruledefs as either for charging, post-processing, or for other purposes. Support to configure a group-of-ruledefs for Traffic Performance Optimization (TPO) in-line service's match-rule and match-advertisement configurations was added to this command.

CLI (ACS Group-of-Ruledefs Configuration Mode)

group-of-ruledefs-application { charging | content-filtering | gx-alias | post-processing | tpo }

no group-of-ruledefs-application

policy-control charging-rule-base-name

This command allows you to configure how the Charging-Rule-Base-Name AVP from PCRF is interpreted, either as ACS rulebase or ACS group-of-ruledefs.

In 12.0 and earlier releases, if multiple Charging-Rule-Base-Name AVP are received from the PCRF, the "last" rulebase is selected and applied to the call. In early 12.2 releases, the "first" rulebase was being selected.

To maintain a uniform behavior, in later 12.2 releases also the "last" rulebase will be selected by default.

In cases where the "first" rulebase has to be selected, a new option "**use-first**" has been introduced.

CLI (ACS Rulebase Configuration Mode)

policy-control charging-rule-base-name { active-charging-group-of-ruledefs | activecharging-rulebase [ignore-when-removed] [use-first]}

default policy-control charging-rule-base-name

no policy-control charging-rule-base-name active-charging-rulebase use-first

pop3 reply args

This command defines rule expressions to match specified arguments with POP3 reply. In this release, the user-specified argument must be 1 through 127 characters in length. In 11.0 and earlier releases, argument must be an alpha and/or numeric string of 1 through 512 characters in length.

CLI (ACS Ruledef Configuration Mode)

[no] pop3 reply args [case-sensitive] *operator argument*

rule-application

This command specifies the purpose of setting up a ruledef as either for charging, post-processing, or for other purposes. Support to configure a ruledef for Traffic Performance Optimization (TPO) in-line service's match-rule and match-advertisement configurations was added to this command.

CLI (ACS Ruledef Configuration Mode)

rule-application { charging | post-processing | routing | tpo }

no rule-application

rule-variable

This command specifies the order of fields in the EDR. The following new fields were added to this command:

- **tcp os-signature**: OS signature string for TCP flow. Enables/disables OS Signature field in EDRs sent to MUR.
- **flow tethered**: Indicates tethering detected on flow. Enables/disables tethering detection result field in EDRs sent to MUR.

CLI (EDR Format Configuration Mode)

rule-variable *protocol rule* **priority** *priority* **[in-quotes]**

no rule-variable *protocol rule* **[priority** *priority* **]**

xheader-insert

This command specifies the extension-header (x-header) format name whose fields are to be inserted in HTTP GET and POST request packets. Support for key encryption was added to this command.

CLI (ACS Charging Action Configuration Mode)

xheader-insert xheader-format *xheader_format_name* **[encryption rc4md5 [encrypted] key** *key* **] [first-request-only] [-noconfirm]**

no xheader-insert

Firewall Commands - Modified in Release 12.0

This section provides information on Stateful Firewall commands modified in Release 12.0.

firewall dos-protection

This command configures Stateful Firewall protection for subscribers from Denial-of-Service (DoS) attacks. The following keywords have been added to this command to support IPv6 firewall:

- **ipv6-dst-options**
- **ipv6-extension-hdrs**
- **ipv6-frag-hdr nested-fragmentation**
- **ipv6-hop-by-hop**

CLI (Firewall-and-NAT Policy Configuration Mode)

[no] firewall dos-protection { all | flooding { icmp | tcp-syn | udp } | ftp-bounce | ip-unaligned-timestamp | ipv6-dst-options [invalid-options | unknown-options] | ipv6-extension-hdrs [limit *extension_limit* **] | ipv6-frag-hdr nested-fragmentation | ipv6-hop-by-hop [invalid-options | jumbo-payload | router-alert | unknown-options] | mime-flood | port-scan | source-router | tcp-window-containment | teardrop | winnuke }**

default firewall dos-protection

firewall ip-reassembly-failure

This command configures Stateful Firewall action on IPv4/IPv6 packets involved in IP Reassembly Failure scenarios. In this release, support for IPv6 firewall is added.

CLI (Firewall-and-NAT Policy Configuration Mode)

firewall ip-reassembly-failure { drop | permit }

default firewall ip-reassembly-failure

firewall max-ip-packet-size

This command configures the maximum IPv4/IPv6 packet size (after IP reassembly) allowed over Stateful Firewall. In this release, support for IPv6 firewall is added.

CLI (Firewall-and-NAT Policy Configuration Mode)

firewall max-ip-packet-size *packet_size* **protocol { icmp | non-icmp }**

default firewall max-ip-packet-size protocol { icmp | non-icmp }

firewall policy

This command enables/disables Stateful Firewall support in a Firewall-and-NAT policy. In this release, support to enable/disable IPv4 and IPv6 firewall is added.

CLI (Firewall-and-NAT Policy Configuration Mode)

firewall policy { ipv4-and-ipv6 | ipv4-only | ipv6-only }

{ default | no } firewall policy

ip max-fragments

This command limits the maximum number of IPv4/IPv6 fragments per fragment chain. In this release, support for IPv6 firewall is added.

CLI (ACS Configuration Mode)

ip max-fragments *max_fragments*

default ip max-fragments

route priority

This command controls routing of packets to protocol analyzers. The **basic-and-advanced** option is added to **sip** keyword for SIP packets to route through SIP analyzer and SIP ALG.

CLI (ACS Rulebase Configuration Mode)

route priority *route_priority* **ruledef** *ruledef_name* **analyzer { dns | file-transfer | ftp-control | ftp-data | h323 | http | imap | mms | p2p | pop3 | pptp | rtcp | rtp | rtsp | sdp | secure-http | sip [advanced | basic-and-advanced] | smtp | tftp | wsp-connection-less | wsp-connection-oriented } [description** *description* **]**

no route priority *route_priority*

Firewall Commands - Modified in Release 12.2

This section provides information on Stateful Firewall commands modified in Release 12.2.

None for this release.

GGSN Commands - Modified in Release 12.0

This section provides information on GGSN commands modified in Release 12.0.

virtual-apn

Virtual APN selection is based on configuration parameters like roaming mode, bearer access service etc. Three more parameters ‘cc-profile’, ‘msisdn-range’, and ‘rat-type’ are added based on them virtual-apn will be selected. ‘CC-profile option specifies the APN for charging characteristics (CC)-profile index. The APN selection will be applied to all subscribers that have msisdn in the configured ‘msisdn-range’. The range has lower and upper limit configured as ‘from’ and ‘to’ respectively. The ‘rat-type’ option configures the APN for rat-type (eutran, gan, geran, hspa, utran, wlan) received in the message.

Another addition is the ‘msin-range from <start_refix> to <end_prefix>’ keywords have been added to the MCC-MNC in this command to enable the IMSI prefix based prepaid/postpaid subscribers selection on GGSN. This enhancement extends the MCC+MNC based virtual APN selection to MCC+MNC+MSIN Range based virtual APN selection.

Virtual APN selection parameter ‘rat-type’ has been enhanced with the inclusion of a new keyword “eutran” along with the utran, geran, wlan, gan, and hspa. It is an enhanced 3GPP standard air interface for LTE mobile networks. Rat-type has also been included as an optional keyword for MCC+MNC.

CLI (APN Configuration Mode)

virtual-apn { gcdr apn-name-to-be-included { gn | virtual } | preference *priority* **apn** *apn_name* **[access-gw-address {** *ip_address* **| ip_address/mask } | bearer-access-service** *svc_name* **| cc-profile** *cc_profile_index* **[rat-type { eutran | gan | geran | hspa | utran | wlan }] | domain** *domain_name* **| mcc** *mcc_number* **mnc** *mnc_number* **[msin-range from** *msin_range_from* **to** *msin_range_to* **| rat-type { eutran | gan | geran | hspa | utran | wlan }] | msisdn-range { from** *msisdn_start_range* **to** *msisdn_to_range* **| rat-type { eutran | gan | geran | hspa | utran | wlan } } | rat-type { eutran | gan | geran | hspa | utran | wlan } | roaming-mode { home | visiting | roaming } } }**

authentication

This command configures the APN’s authentication parameters. A new option ‘prefer-chap-pco’ has been added to be used along with msisdn-auth/imsi-auth parameter. With this option, if enabled, GGSN performs CHAP authentication if CHAP parameters are received in Protocol Configuration Options (PCO). However, chap username would be constructed as *msisdn@apn / imsi@apn* and chap challenge, chap response parameters should be used as it is from CHAP parameters received in PCO IE. If CHAP parameters are not received in PCO IE of CPC Request, GGSN should do normal PAP authentication with PAP username as *msisdn@apn / imsi@apn* (ignoring any PAP username if received).

Another new mandatory keyword “pco-username” has been added for “allow-noauth”. This option allows session to get establish when PCO contains both “PAP” and “CHAP” in authentication disabled state.

IMPORTANT

This change is applicable for 10.2 and above versions.

CLI (APN Configuration Mode)

```
authentication { [ msid-auth | imsi-auth [ password-use-pco |
username-strip-apn | prefer-chap-pco ] | msisdn-auth [ password-use-pco |
username-strip-apn | prefer-chap-pco ] | eap initial-access-request [
authenticate-authorize | authenticate-only ] | [ allow-noauth [
pco-username { chap | pap } ] [ chap preference [ convert-to-mschap ] ] [
mschap preference] [ pap preference ] }
```

ip user-datagram-tos copy

This command controls copying of IP TOS octet value from user IPv4/IPv6 datagrams to header of GTP tunnel encapsulation. Earlier the “data-tunnel” option appeared after this command, but it was removed to match with the same command in Subscriber Configuration Mode command.

CLI (APN Configuration Mode)

```
[ no | default ] ip user-datagram-tos copy
```

crypto ipsec transform-set

From the Context Configuration Mode, this command creates IPSec transform sets. A new aes-cbc-256 cipher has been added to the existing list of supported cipher options.

CLI (Context Configuration Mode)

```
[ no ] crypto ipsec transform-set transform_name [ ah { hmac { md5-96 | none
| sha1-96 } { esp { hmac { { md5-96 | sha1-96 } { cipher { 3des-cbc |
aes-cbc-128 | aes-cbc-256 | des-cbc } } | none } } } } ]
```

sgsn mcc-mnc

From the GGSN Service Configuration Mode, the `sgsn` command configures the SGSNs allowed to connect to this GGSN. A new option ‘`mcc-mnc`’ has been added to this command to configure the sgsn mcc-mnc to the GGSN service. This implementation gives first preference to “User Location Information” IE in Create PDP Context Request Message (to be sent to PCRF) for determining 3GPP-SGSN-MCC-MNC attribute. For backward compatibility with this old behavior, CLI controlled implementation has been done so that existing deployments are not affected with this change in behavior.

CLI (GGSN Service Configuration Mode)

```
sgsn mcc-mnc { prefer rai | prefer uli }
```

```
default sgsn mcc-mnc
```

GGSN Commands - Modified in Release 12.2

This section provides information on GGSN commands modified in Release 12.2.

gtpp storage-server local file

This command configures the parameters for GTPP files stored locally on GTPP storage server. A new option “start-file-seq-num” has been added to this command from 12.2 onwards which will allow the operators to configure the start file sequence number at the specified value and go on incrementing until the maximum sequence number configured in the file format is reached and then it would rollover.

In case the optional value “Recover-file-seq-num” is configured then every time the machine is rebooted (or aaaproxy recovery/planned/Unplanned PSC migration) the file sequence number continues from the last sequence and goes on incrementing until the maximum sequence number configured in file name format is reached and then it would rollover and start from the start-file-seq-num value.

CLI (Context Configuration Mode)

gtpp storage-server local file { **compression** { **gzip** | **none** } | **format** { **custom1** | **custom2** | **custom3** | **custom4** | **custom5** | **custom6** | **custom7** | **custom8** } | **name** { **format** *string* [**max-file-seq-num** *seq_number*] | **prefix** *prefix* } | **purge-processed-files** [**file-name-pattern** *file_pattern* | **purge-interval** *purge_dur*] | **rotation** { **cdr-count count** | **time-interval** *time* [**force-file-rotation**] | **volume mb** *size* } | **start-file-seq-num** *seq_num* [**recover-file-seq-num**] }

default gtpp storage-server local file { **compression** | **format** | **name** { **format** | **prefix** } | **purge-processed-files** | **rotation** { **cdr-count** | **time-interval** | **volume** } | **start-file-seq-num** }

gtpp trigger

This command disables GTPP trigger conditions that cause either partial CDR record closure or opening of new CDR record container. GTPP triggers are specified in 3GPP TS 32251 v6.6.0. The CDRs that are generated due to uli-change are increasing the CDR traffic and therefore a new keyword “uli-change” has been added to this command to have one configurable CLI that can control the enabling/disabling of these triggers.

CLI (GTPP Group Configuration Mode)

gtpp trigger { cell-update | direct-tunnel | egcdr max-losdv | ggsn-preservation-mode-change | inter-plmn-sgsn-change | ms-timezone-change | plmn-id-change | qos-change | rat-change [generate { cdr | container }] | routing-area-update | sgsn-change-limit | serving-node-change-limit | tariff-time-change | time-limit | uli-change | volume-limit }

default gtpp trigger

no gtpp trigger { cell-update | direct-tunnel | egcdr max-losdv | ggsn-preservation-mode-change | inter-plmn-sgsn-change | ms-timezone-change | plmn-id-change | qos-change | rat-change | routing-area-update | sgsn-change-limit | serving-node-change-limit | tariff-time-change | time-limit | uli-change | volume-limit }

authentication

This command configures the APN authentication parameters. A new optional keyword “convert-to-mschap” has been added with CHAP option of this command. With this enhancement, the CHAP parameters with the length of 49 bytes are converted to MSCHAP by AAAmgr. If this new keyword is disabled, the CHAP is not converted to MSCHAP even if CHAP parameter length is 49 bytes.

CLI (APN Configuration Mode)

```
authentication [ [ msid-auth | imsi-auth [ password-use-pco |
username-strip-apn | prefer-chap-pco ] | msisdn-auth [ password-use-pco |
username-strip-apn | prefer-chap-pco ] | eap initial-access-request [
authenticate-authorize | authenticate-only ] | [ allow-noauth ] [ chap
preference [ convert-to-mschap ] ] [ mschap preference ] [ pap preference ]
]
```

gtpp dictionary

This command designates a specific dictionary used by GTPP for a specific context. A new set of dictionaries from custom 41 to custom 60 has been created for all products and necessary support to be provided.

CLI (GTPP Group Configuration Mode)

```
gtpp dictionary { custom1 | custom10 | custom11 | custom12 | custom13 |
custom14 | custom15 | custom16 | custom17 | custom18 | custom19 | custom2 |
custom20 | custom21 | custom22 | custom23 | custom24 | custom25 | custom26
| custom27 | custom28 | custom29 | custom3 | custom30 | custom31 | custom32
| custom33 | custom34 | custom35 | custom36 | custom37 | custom38 |
custom39 | custom4 | custom40 | custom41 | custom42 | custom43 | custom44 |
custom45 | custom46 | custom47 | custom48 | custom49 | custom5 | custom50 |
custom51 | custom52 | custom53 | custom54 | custom55 | custom56 | custom57
| custom58 | custom59 | custom6 | custom60 |  custom7 | custom8 | custom9 |
standard }
```

HA Commands - Modified in Release 12.0

This section provides information on HA commands modified in Release 12.0.

None for this release.

aaa accounting [roaming]

The following commands have been modified in Release 12.2.

Below command enables the sending of AAA accounting information by the Home Agent

Key word **roaming** is added in the below command

CLI (HA Service Config Mode)

```
aaa accounting [ roaming ]
```

aaa accounting [roaming]

The following commands have been modified in Release 12.2.

Below command enables the sending of AAA accounting information by the LNS

Key word **roaming** is added in the below command

CLI (LNS Service Config Mode)

aaa accounting [roaming]

radius probe-message

The following commands have been modified in 12.2

Below command configures the service ip-address to be sent as an AVP in RADIUS authentication probe messages.

CLI (Context Configuration Mode)

radius probe-message local-service-address *ipv4/ipv6_address*

HSGW Commands - Modified in Release 12.0

This section provides information on HSGW commands modified in Release 12.0.

None for this release.

HSGW Commands - Modified in Release 12.2

This section provides information on HSGW commands modified in Release 12.2.

information-element-set

The keyword **custom2** and its options have been added to the following command.

CLI (MAG Service Configuration Mode)

information-element-set { custom1 | custom2 | standard }

default information-element-set

ipv6 initial-router-advt

The keyword **router-solicit-wait-timeout** and its options have been added to the following command.

CLI (Subscriber Configuration Mode)

ipv6 initial-router-advt { interval *value* **| num-advts** *value* **| router-solicit-wait-timeout** *value* **}**

default ipv6 initial-router-advt { interval | num-advts | router-solicit-wait-timeout }

no ipv6 initial-router-advt router-solicit-wait-timeout

IPCF Commands - Modified in Release 12.1

This section provides information on modified IPCF commands in Release 12.1.

IPCF is a new product for this release.

IPSG Commands - Modified in Release 12.2

This section provides information on modified IPSG commands in Release 12.2.

radius accounting

This command specifies the IP address and shared secret of the RADIUS accounting client from which RADIUS accounting requests are received. The maximum value for the keyword **encrypted key** has been changed from 127 to 236 characters.

CLI (IPSG RADIUS Server Configuration Mode)

radius accounting { { client { *ipv4/ipv6_address* | *ipv4/ipv6_address/mask* **}** **[encrypted] key** *secret* **[dictionary** *dictionary* **] [disconnect-message [** **dest-port** *destination_port* **]] } | { interim create-new-call } }**

Mobility Management Entity Commands - Modified in Release 12.0

This section provides information on MME commands modified in Release 12.0.

apn-selection-default

The **apn-selection-default** command enables and configures the Default APN feature for use when the normal APN selection process fails. A new keyword, **first-in-subscription**, has been added in this release and specifies that the first APN in the subscription record matching the PDN type is used if the UE APN is absent and the default APN is not a match.

CLI (APN Remap Table Configuration Mode)

apn-selection-default { first-in-subscription | network-identifier *apn_net_id* **[fallback-apn** *apn_net_id* **| reject-blank-apn |** **require-dns-fail-wildcard | require-subscription-apn] }**

associate

The **associate** command configures association between the MME service and other services such as the HSS peer service and the SGs service. An **sctp-param-template** keyword and associated variable has been added to this command. The **sctp-param-template** keyword allows the MME service to be associated with a configured SCTP parameter template. SCTP parameter templates are configured through the Global Configuration Mode.

Also, the **associate sgs-service** command now allows the SGs context to be configured.

CLI (MME Service Configuration Mode)

associate { { egtp-service *egtp_svc_name* **| hss-peer-service** *hss_svc_name* **|** **sctp-param-template** *template_name* **| sgs-service** *sgs_svc_name* **|**

sgtpc-service *sgtpc_svc_name* **} [context** *ctx_name* **] | subscriber-map** *map_name* **| tai-mgmt-db** *database_name* **}**

attach

The **attach** command now supports the ability of the MME to allow call processing even if the EIR check times out. Also, the MME now has the ability to allow call processing on emergency verification. The addition of the **allow-on-eca-timeout** keyword provides this function.

CLI (Call Control Profile Configuration Mode)

attach imei-query-type { imei | imei-sv | none } [verify-equipment-identity [allow-on-eca-timeout | deny-greylisted | deny-unknown]]

authenticate

The **authenticate** command enables authentication for a variety of procedures within services using the configure call control profile. The authentication of SMS procedures has been added in this release.

CLI (Call Control Profile Configuration Mode)

authenticate sms [access-type { gprs | umts } | frequency frequency | sms-type { mo-sms | mt-sms }]

bind s1-mme

The **bind s1-mme** command connects the MME service to the S1-MME interface. In this release, the ability to configure node-to-node IP security has been added. An optional **crypto template** keyword and associated variable has been added to this command.

CLI (MME Service Configuration Mode)

bind s1-mme ipv4-address *address* **[ipv4-address** *secondary_address* **] | ipv6-address** *address* **[ipv6-address** *secondary_address* **] } [crypto-template** *name* **] [max-subscribers** *number* **]**

IMPORTANT

Crypto templates can only be associated with IPv4 addresses on the S1-MME in this release.

dns

The **dns** command configures association between the MME service and a named context where a DNS client resides allowing for DNS queries to peer servers or other EPC entities. An **peer-sgsn** keyword has been added to this command. The **peer-sgsn** keyword allows the MME service to be associated with a context where a DNS client provides DNS queries to locate a peer SGSN.

CLI (MME Service Configuration Mode)

dns { peer-mme | peer-sgsn | pgw | sgw | [context *ctx_name* **]**

policy attach

The **policy attach** command now supports the ability of the MME to allow call processing even if the EIR check times out. Also, the MME now has the ability to allow call processing on emergency verification. The addition of the **allow-on-eca-timeout** keyword provides this function.

CLI (MME Service Configuration Mode)

```
policy attach { imei-query-type { imei | imei-sv | none } [
verify-equipment-identity [ allow-on-eca-timeout | deny-greylisted |
deny-unknown ] ] | set-ue-time { disable | enable }
```

policy tau

The **policy tau** command now supports the ability of the MME to allow call processing even if the EIR check times out. Also, the MME now has the ability to allow call processing on emergency verification. The addition of the **allow-on-eca-timeout** keyword provides this function.

CLI (MME Service Configuration Mode)

```
policy tau { imei-query-type { imei | imei-sv | none } [
verify-equipment-identity [ allow-on-eca-timeout | deny-greylisted |
deny-unknown ] ] | set-ue-time { disable | enable }
```

tau

The **tau** command now supports the ability of the MME to allow call processing even if the EIR check times out. Also, the MME now has the ability to allow call processing on emergency verification. The addition of the **allow-on-eca-timeout** keyword provides this function.

CLI (Call Control Profile Configuration Mode)

```
tau { imei-query-type { imei | imei-sv | none } [ verify-equipment-identity
[ allow-on-eca-timeout | deny-greylisted | deny-unknown ] ] | inter-rat
security-ctxt { allow-mapped | native } }
```

Mobility Management Entity Commands - Modified in Release 12.2

This section provides information on MME commands modified in Release 12.2.

associate

The **associate** command now allows the MME service to associate with the global MME ID management database.

CLI (MME Service Configuration Mode)

associate { { egtp-service *egtp_svc_name* **| egtp-sv-service** *egtp_sv_svc_name* **| hss-peer-service** *hss_svc_name* **| lte-emergency-profile** *profile_name* **| network-global-mme-id-mgmt-db | sctp-param-template** *template_name* **| sgs-service** *sgs_svc_name* **| sgtpc-service** *sgtpc_svc_name* **} [context** *ctx_name* **] | subscriber-map** *map_name* **| tai-mgmt-db** *database_name* **}**

attach

The **attach** command now supports the ability of the MME to allow call processing even if the EIR check times out. Also, the MME now has the ability to allow call processing on emergency verification. The addition of the **allow-on-eca-timeout** and the **verify-emergency** keywords provide these functions.

CLI (Call Control Profile Configuration Mode)

attach imei-query-type (imei | imei-sv | none) [verify-equipment-identity [allow-on-eca-timeout | deny-greylisted | deny-unknown | verify-emergency]]

bind

The **bind** command now supports IPv6 addressing as well as SCTP multi-homing with the addition of the secondary **ipv4-address** keyword and the initial and secondary **ipv6-address** keywords.

CLI (MME SGs Service Configuration Mode)

bind (ipv4-address *ipv4_address* **[ipv4-address** *ipv4_address* **] | ipv6-address** *ipv6_address* **[ipv6-address** *ipv6_address* **] }**

cc

The **cc prefer** command now supports the ability of the MME to use charging characteristics from an HSS or by using locally set values. This, in conjunction with the addition of the time zone mapping command, supports TAI based UE time zone reporting by the MME so it can be passed to the S-GW and P-GW to be included as the UE time zone in billing records.

CLI (Call Control Profile Configuration Mode)

cc { behavior-bit no-records *bit_value* **| local-value behavior** *bit_value* **profile** *index_bit* **| prefer { hlr-hss-value | local-value } }**

clear subscribers mme-service

The **clear subscribers mme-service** command now supports the ability to clear individual PDNS or bearers based on the EPS bearer identity.

CLI (Exec Mode)

clear subscribers mme-service *name* **ebi** *num*

diameter-result-code-mapping

Previously the MME supported configuration of NAS cause codes to signal to the UE when the MME receives a diameter result code of 5421 (RAT not allowed) from the HSS. The following EMM cause codes were previously supported for this use:

"#15 "No suitable cells in tracking area", or

"#13 "Roaming not allowed in this tracking area", or

"#12 "Tracking area not allowed"

In this release, the following additional diameter result codes are now also supported. The following table also lists the EMM cause codes to which each diameter result code is mapped by default.

Table 3-1 Diameter Result Codes

Diameter Result Code	Default Cause Code Signaled to the UE
DIAMETER_ERROR_USER_UNKNOWN (5001) (experimental result code) DIAMETER_ERROR_USER_UNKNOWN (5030)	#8 "EPS services and non-EPS services not allowed"
DIAMETER_ERROR_UNKNOWN_EPS_ SUBSCRIPTION (5420)	#15 "No suitable cells in tracking area"
DIAMETER_ERROR_ROAMING_NOT_ALLOWED (5004)	#11 "PLMN not allowed"
DIAMETER_AUTHORIZATION_REJECTED (5003)	#15 "No suitable cells in tracking area"
DIAMETER_UNABLE_TO_COMPLY (5012)	#17 "Network failure"
DIAMETER_INVALID_AVP_VALUE (5004)	#17 "Network failure"
DIAMETER_UNSUPPORTED_FEATURE (5011)	#15 "No suitable cells in tracking area"
Any code that is not specified above	#17 "Network failure".

These mappings can be altered using the following CLI command.

CLI (Call Control Configuration Mode)

diameter-result-code-mapping s6a *diameter_result_code* **mme-emm-cause** *emm_cause_code*

enb-cache-timeout

The maximum configurable value for eNodeB cache timeout has been increased from 60 minutes to 1440 minutes.

CLI (MME Service Configuration Mode)

enb-cache-timeout *min*

gtpc

The following keyword has been added to this command to configure the MME to include the preamble in the target-id of relocation requests that it sends:

- **target-identification-preamble**

By default, it does not include the preamble.

CLI (SGTP Service Configuration Mode)

gtpc { bind address *ip_address* | **dns-sgsn context** *cntxt_name* | **echo-interval** *seconds* | **guard-interval** *seconds* | **ignore response-port-validation** | **ip qos-dscp** *<dscp_marking>* | **max-retransmissions** *num* | **retransmission-timeout** *seconds* | **send { common flags** | **rab-context** | **target-identification-preamble } }**

no gtpc { bind address *ip_address* | **dns-sgsn context** *cntxt_name* | **echo-interval** *seconds* | **send { commo- flags** | **rab-context** | **target-identification-preamble} }**

default gtpc { echo-interval | **guard-interval** | **ignore response-port-validation** | **ip qos-dscp** | **max-retransmissions** | **retransmission-timeout** | **send { commonflags** | **rab-context** | **target-identification-preamble } }**

non-pool-area

To support enhanced TAI to LAI mapping, the **non-pool-area** command now supports the optional configuration of the Public Land Mobile Network (PLMN) ID to determine the correct VLR to use, by including the optional **plmnid** keywords.

CLI (MME SGs Service Configuration Mode)

non-pool-area *name* **use-vlr** *vlr_name* **[lac** *value(s)* **] [plmnid { any** | **mcc** *mcc_value* **mnc** *mnc_value* **}]**

policy attach

The **policy attach** command now supports the ability of the MME to allow call processing even if the EIR check times out. Also, the MME now has the ability to allow call processing on emergency verification. The addition of the **allow-on-eca-timeout** and the **verify-emergency** keywords provide these functions.

CLI (MME Service Configuration Mode)

policy attach { imei-query-type (imei | **imei-sv** | **none) [verify-equipment-identity [allow-on-eca-timeout** | **deny-greylisted** | **deny-unknown** | **verify-emergency]]** | **set-ue-time (disable** | **enable }**

policy inter-rat

This command now includes an **ignore-sgsn-context-id** keyword option which configures the MME to ignore Context-Identifier mismatches between the HSS and HLR for a given subscriber. If enabled, the MME uses the Context-ID from the HSS to override the Context-ID from the HLR. If this option is disabled (default), the MME will drop the PDN when there is a Context-ID mismatch.

MME Service Configuration Mode

policy inter-rat { ignore-sgsn-context-id | **indirect-forwarding-tunnels always }**

policy network

The **policy network** command now supports the ability to switch on dual-addressing support to all network nodes including pre-release 8 SGSNs (Gn/Gp).

CLI (MME Service Configuration Mode)

policy network dual-addressing-supported

policy tau

The **policy tau** command now supports the ability of the MME to allow call processing even if the EIR check times out. Also, the MME now has the ability to allow call processing on emergency verification. The addition of the **allow-on-eca-timeout** and the **verify-emergency** keywords provide these functions.

CLI (MME Service Configuration Mode)

policy tau { imei-query-type { imei | imei-sv | none } [verify-equipment-identity [allow-on-eca-timeout | deny-greylisted | deny-unknown | verify-emergency]] | set-ue-time (disable | enable }

vlr

The **vlr** command now supports IPv6 addressing as well as SCTP multi-homing with the addition of the secondary **ipv4-address** keyword and the initial and secondary **ipv6-address** keywords.

CLI (MME SGs Service Configuration Mode)

vlr *vlr_name* **(ipv4-address** *ipv4_address* **[ipv4-address** *ipv4_address* **] | ipv6-address** *ipv6_address* **[ipv6-address** *ipv6_address* **] } port** *port_number*

tau

The **tau** command now supports the ability of the MME to allow call processing even if the EIR check times out. Also, the MME now has the ability to allow call processing on emergency verification. The addition of the **allow-on-eca-timeout** and the **verify-emergency** keywords provide these functions.

CLI (Call Control Profile Configuration Mode)

tau { imei-query-type { imei | imei-sv | none } [verify-equipment-identity [allow-on-eca-timeout | deny-greylisted | deny-unknown | verify-emergency]] | inter-rat security-ctxt { allow-mapped | native } }

NAT Commands - Modified in Release 12.0

This section provides information on NAT commands modified in Release 12.0.

firewall nat-alg

This command enables/disables all or specified NAT Application Level Gateways (ALG). The **h323** keyword is added to this command to enable/disable H323 processing.

CLI (ACS Configuration Mode)

[default | no] firewall nat-alg { all | ftp | h323 | pptp | rtsp | sip }

route priority

This command controls routing of packets to protocol analyzers. The **h323** keyword is added to this command to route the H323 analyzer for the ruledef.

CLI (ACS Rulebase Configuration Mode)

route priority *route_priority* **ruledef** *ruledef_name* **analyzer { dns | file-transfer | ftp-control | ftp-data | h323 | http | imap | mms | p2p | pop3 | pptp | rtcp | rtp | rtsp | sdp | secure-http | sip [advanced] | smtp | tftp | wsp-connection-less | wsp-connection-oriented } [description** *description* **]**

no route priority *route_priority*

NAT Commands - Modified in Release 12.2

This section provides information on NAT commands modified in Release 12.2.

firewall nat-alg

This command enables/disables all or specified NAT Application Level Gateways (ALG). The following keywords are added to this command to enable/disable processing for NAT44/NAT64 ALGs.

- **ipv4-and-ipv6**
- **ipv4-only**
- **ipv6-only**

CLI (ACS Configuration Mode)

[default | no] firewall nat-alg { all | ftp | h323 | pptp | rtsp | sip } [ipv4-and-ipv6 | ipv4-only | ipv6-only]

nat policy

This command enables/disables Network Address Translation (NAT) support in a Firewall-and-NAT policy. The following keywords are added to this command to enable/disable NAT processing for IPv4/IPv6:

- **ipv4-and-ipv6**
- **ipv4-only**
- **ipv6-only**

CLI (Firewall-and-NAT Policy Configuration Mode)

nat policy [ipv4-and-ipv6 | ipv4-only | ipv6-only] [default-nat-realm *nat_realm_name* **[fw-and-nat-action** *action_name* **]]**

no nat policy

route priority

This command controls routing of packets to protocol analyzers. The **basic-and-advanced** option is added to **sip** keyword for SIP packets to route through SIP analyzer and SIP ALG.

CLI (ACS Rulebase Configuration Mode)

route priority *route_priority* **ruledef** *ruledef_name* **analyzer { dns | file-transfer | ftp-control | ftp-data | h323 | http | imap | mms | p2p | pop3 | pptp | rtcp | rtp | rtsp | sdp | secure-http | sip [advanced |**

basic-and-advanced] | smtp | tftp | wsp-connection-less | wsp-connection-oriented } [description *description* **]**

no route priority *route_priority*

Packet Data Network Gateway Commands - Modified in Release 12.0

This section provides information on P-GW commands modified in Release 12.0.

diameter

The keyword **service-context-id** has been added to this command.

CLI (Credit Control Configuration Mode)

diameter service-context-id *service_context_id*

default diameter service-context-id

gtpp attribute

This command enables the specification of some of the optional fields in the CDRs that the GSN (GGSN, P-GW, or SGSN) generates and/or how the information is to be presented. Several keywords have been added.

CLI (GTPP Server Group Configuration Mode)

gtpp attribute { camel-info | cell-plmn-id | diagnostics | duration-ms | imei | local-record-sequence-number | msisdn | node-id-suffix *STRING* **| plmn-id | rat | record-extensions rat | sms { destination-number | recording-entity | service-centre } } +**

default gtpp attribute { cell-plmn-id | diagnostics | duration-ms | imei | local-record-sequence-number | msisdn | plmn-id | rat | record-extensions rat | sms { destination-number | recording-entity | service-centre } }

no gtpp attribute { cell-plmn-id | diagnostics | duration-ms | imei | local-record-sequence-number | msisdn | node-id-suffix | plmn-id | rat | record-extensions rat | sms { destination-number | recording-entity | service-centre } }

gtpp egcdr

The keyword **rulebase-max-length** and its options have been added to the following command.

CLI (Context Configuration Mode)

CLI (GTPP Group Configuration Mode)

gtpp egcdr { final-record [[include-content-ids { all | only-with-traffic }] [closing-cause { same-in-all-partials | unique }]] | losdv-max-containers *max_losdv_containers* **| lotdv-max-containers** *max_lotdv_containers* **| rulebase-max-length** *rulebase_name_max_length* **| service-data-flow threshold { interval** *interval* **| volume { downlink** *bytes* **[uplink** *bytes* **] | total** *bytes* **| uplink** *bytes* **[downlink** *bytes* **] } } | service-idle-timeout { 0 |** *service_idle_timeout* **} }**

default gtpp egcdr { final-record include-content-ids only-with-traffic closing-cause same-in-all-partials | losdv-max-containers | lotdv-max-containers | service-idle-timeout 0 }

no gtpp egcdr { rulebase-max-length | service-data-flow threshold { interval | volume { downlink [uplink] | total | uplink [downlink] } } }

ikev2-ikesa

The following keywords and their options have been added to the following command.

- allow-empty-ikesa
- retransmission-timeout
- transform-set

CLI (ACS x-header Format Configuration Mode)

ikev2-ikesa { allow-empty-ikesa | max-retransmissions *number* **| rekey | retransmission-timeout** *msec* **| setup-timer** *sec* **| transform-set list** *name* **}**

default ikev2-ikesa { allow-empty-ikesa | max-retransmissions | rekey | setup-timer }

no ikev2-ikesa { allow-empty-ikesa | rekey | transform-set list }

insert

Support has been added for the following **charging-characteristics**:

- Service Data Volume Limit
- Service Data Time Limit

CLI (ACS x-header Format Configuration Mode)

insert *xheader_field_name* **{ string-constant** *xheader_field_value* **| variable { bearer { 3gpp { apn | charging-characteristics | charging-id | imei | imsi | rat-type | sgsn-address } | acr | customer-id | ggsn-address | mdn | radiuscalling-station-id | session-id | sn-rulebase| subscriber-ip-address | username } [encrypt] | http { host | url } }**

no insert *xheader_field_name*

trigger type

Support has been added for **serving-node** trigger type.

CLI (Credit Control Configuration Mode)

[no] trigger type { cellid | lac | qos | rat | serving-node | sgsn } +

default trigger type

Packet Data Network Gateway Commands - Modified in Release 12.2

This section provides information on P-GW commands modified in Release 12.2.

apn-ambr

The keyword **shape** and its options have been removed from the following command.

CLI (APN Configuration Mode)

Previous:

apn-ambr rate-limit direction { downlink | uplink } [burst-size { auto-readjust duration *seconds* **|** *bytes* **} | violate-action { drop | lower-ip-precedence | shape [transmit-when-buffer-full] | transmit }]**

[default | no] apn-ambr rate-limit direction { downlink | uplink }

Now:

apn-ambr rate-limit direction { downlink | uplink } [burst-size { auto-readjust duration *seconds* **|** *bytes* **} | violate-action { drop | lower-ip-precedence | transmit }]**

[default | no] apn-ambr rate-limit direction { downlink | uplink }

P-GW does not support traffic shaping for APN-AMBR.

cc

The following keywords have been added to this command:

- **sdf-interval**
- **sdf-volume**

CLI (Accounting Policy Configuration Mode)

cc profile *index* **{ buckets** *num* **| interval** *seconds* **| sdf-interval** *seconds* **| sdf-volume { downlink** *octets* **{ uplink** *octets* **} | total** *octets* **| uplink** *octets* **{ downlink** *octets* **} } | serving-nodes** *num* **| tariff time1** *min hrs* **[time2** *min hrs***...time4** *min hrs* **] | volume { downlink** *octets* **{ uplink** *octets* **} | total** *octets* **| uplink** *octets* **{ downlink** *octets* **} } }**

default cc profile *index*

no cc profile *index* **{ buckets | interval | sdf-interval | sdf-volume | serving-nodes | tariff | volume }**

virtual-apn

Old Behavior:

With previous **virtual-apn** CLI command, either cc or imsi could be used to define a selection rule for virtual apn.

New Behavior:

Now, **virtual-apn** CLI command can also be used to define a imsi+cc virtual apn selection rule.

CLI (APN Configuration Mode)

virtual-apn { gcdr apn-name-to-be-included { Gn | virtual } | preference *priority* **apn** *apn_name* **[access-gw-address {** *ip_address* **|** *ip_address/mask* **} | bearer-access-service** *svc_name* **| cc-profile** *cc_profile_index* **[rat-type { eutran | gan | geran | hspa | utran | wlan }] | domain** *domain_name* **| mcc** *mcc_number* **mnc** *mnc_number* **[cc-profile** *cc_profile_index* **] | [msin-range from** *msin_range_from* **to** *msin_range_to* **] | [rat-type { eutran | gan | geran | hspa | utran | wlan }] | msisdn-range { from** *msisdn_start_range* **to** *msisdn_to_range* **| rat-type { eutran | gan | geran | hspa | utran | wlan } }**

```
| rat-type { eutran | gan | geran | hspa | utran | wlan } | roaming-mode {
home | roaming | visiting } ] }
```

```
default virtual-apn gcdr apn-name-to-be-included
```

```
no virtual-apn preference priority
```

PDIF Commands - Modified in Release 12.0

This section provides information on PDIF commands modified in Release 12.0.

None for this release.

PDSN Commands - Modified in Release 12.0

This section provides information on PDSN commands modified in Release 12.0.

neighbor fall-over bfd multihop

The following keyword has been added to the command.

- fall-over bfd multihop

CLI (Router bgp Mode)

```
[ no ] neighbor ip_address fall-over bfd multihop
```

neighbor password / encrypted password

The following keywords have been added to the command.

- password
- encrypted password

CLI (Router bgp Mode)

```
neighbor ip_addres password password
```

```
neighbor ip_addres encrypted password encrypted_password
```

```
[ no ] neighbor ip_addres password
```

neighbor srp-activated-soft-clear

The following keyword has been added to the command.

- srp-activated-soft-clearp

CLI (Router bgp Mode)

```
[ no ] neighbor ip_address srp-activated-soft-clear
```

show rp statistics pcf-summary

The following keyword has been added to the command.

- pcf-summary

CLI (Config Mode)

```
show rp statistics pcf-summary
```

Serving Gateway Commands - Modified in Release 12.0

This section provides information on commands modified in Release 12.0.

associate

The associate command in the S-GW Service Configuration Mode is updated with the new **subscriber-map** keyword. This new keyword allows the S-GW service to be associated with a subscriber map configured through the LTE Policy Configuration Mode, and thus, to an operator policy.

CLI (S-GW Service Configuration Mode)

associate subscriber-map *name*

cc

The S-GW now supports the charging characteristics (**cc**) commands in the APN Profile and Call Control Profile Configuration Modes.

CLI (APN Profile Configuration Modes)

cc { local-value-for-scdrs behavior *bit_value* **profile** *index_bit* **| prefer { hlr-value-for-scdrs | local-value-for-scdrs } }**

CLI (Call Control Profile Configuration Modes)

cc { behavior-bit no-records *bit_value* **| local-value behavior** *bit_value* **profile** *index_bit* **| prefer { hlr-value | local-value } }**

accounting context

The S-GW now supports the accounting context command in the Call Control Profile Configuration Mode.

CLI (S-GW Service Configuration Mode)

accounting context ctxt_name [*gtpp group grp_name* **]**

Session Control Manager Commands - Modified in Release 12.0

This section provides information on SCM commands modified in Release 12.0.

authorization

This command functionality has been moved from the CSCF Proxy-CSCF Configuration Mode and expanded.

CLI (CSCF PCRF-Policy-Control Configuration Mode)

[no] authorization mediatype { application | audio | control | data | message | others | text | video }

bind

The keyword **tls-crypto-template** and its options have been added to this command.

CLI (CSCF Service Configuration Mode)

bind address ip_address [cscf-hostname *host_name* **] [ipsec-crypto-template** *template* **] [max-sessions** *max#* **] [port** *number* **] [reserved-call-capacity** *percentage* **] [tls-crypto-template** *template* **[tls-port** *number* **]] [transport tcp] [use-serviceport-towards-network]**

no bind address

nat-pool

The keyword **signalling-pool** has been added to this command. Specifies the name of an existing IP pool from where IP addresses will be used to fill in signalling headers only.

CLI (CSCF Service Configuration Mode)

nat-pool name *pool_name* **[signalling-pool** *signalling_pool_name* **]**

no nat-pool name *pool_name*

policy

The keyword **overload** and its options have been moved from the CSCF Policy Rules Configuration Mode. The keyword **ibcf-capability** has also been added to this command.

CLI (CSCF Service Configuration Mode)

policy { accounting interim-interval *value* **| allow-early-media | ibcf-capability domain** *domain/name* **| overload [drop | redirect** *IPv4_address1* **[weight** *weight1* **] [** *IPv4_address2* **[weight** *weight2* **]] ... | reject] | threshold congestion-control { system-cpu-utilization** *percent* **| tolerance** *percent* **} }**

default policy { allow-early-media | overload | threshold congestion-control { system-cpu-utilization | tolerance } }

no policy { accounting interim-interval | allow-early-media | ibcf-capability domain *domain/name* **| overload [redirect** *IPv4_address1* **] [** *IPv4_address2* **] ... | threshold congestion-control { system-cpu-utilization | tolerance } }**

threshold

This command enables thresholds alerting and configuration of thresholds for CSCF Service. This functionality has been moved from the Global Configuration Mode.

CLI (CSCF Service Configuration Mode)

threshold { { call-setup-failures | call-total-active | error-no-resource | error-presence | error-reg-auth | error-tcp | invite-rcvd-rate | reg-rcvd-rate | reg-total-active | route-failures } *high_thresh* **[clear** *low_thresh* **] | monitoring }**

[default | no] monitoring

timeout

The keyword **cleanup-timer** has been added to this command. This timer is used to control how often to check for idle TCP connections.

CLI (CSCF Service Configuration Mode)

timeout { hss-wait *sec* **| no-answer** *sec* **| policy-interface** *sec* **| sip { 3gpp-d** *sec* **| 3gpp-t1** *msec* **| 3gpp-t2** *sec* **| 3gpp-t4** *sec* **| d** *sec* **| idle-tcp-connection** *msec* **[cleanup-timer** *msec* **] | invite-expiry** *sec* **| t1** *msec* **| t2** *sec* **| t4** *sec* **} }**

default timeout { hss-wait | no-answer | policy-interface | sip { 3gpp-d | 3gpp-t1 | 3gpp-t2 | 3gpp-t4 | d | idle-tcp-connection | invite-expiry | t1 | t2 | t4 } }

trusted-domain-entity

The keyword **private-network** has been added to this command.

CLI (CSCF Service Configuration Mode)

trusted-domain-entity *address* **[foreign-network] [private-network]**

no trusted-domain-entity *address*

Session Control Manager Commands - Modified in Release 12.2

This section provides information on SCM commands modified in Release 12.2.

aaa-group

The keyword **source** has been removed from the following command.

In addition, the keyword **preference** and its options have been added to this command.

CLI (CSCF Diameter Selection Configuration Mode)

Previous:

aaa-group *name* **criteria { source aor** *aor_prefix* **| subscriber-capability { audio [only] | text | video } | subscriber-ip-type { v4 | v6 } } +**

no aaa-group *name*

Now:

aaa-group *name* **{ [preference** *value* **] criteria { aor** *aor_prefix* **| subscriber-capability {** *capability_type* **} | subscriber-ip-type { v4 | v6 } } + }**

no aaa-group *name* **preference** *value*

Previously, if **criteria source aor <***aor-prefix***>** was configured, fetching of aaa group name was done based on source aor. Now, fetching of aaa group name for a subscriber can be based on source aor match or destination aor match.

action

The keyword **length** and its options have been added to this command.

CLI (CSCF URI Readdress Configuration Mode)

action modify *string* **position** *num* **length** *length* **target { destination | source } { aor | domain | user }**

no action

authentication

The keyword **custom-md5** has been added to this command:

CLI (CSCF Access Profile Configuration Mode)

[no] authentication { aka-v1 | custom-md5 | md5 }

authentication

The following keywords and their options have been added to this command:

- **allow-auth-rsp-failure**
- **allow-hss-failure**
- **allow-skip-sar**
- **custom-md5**
- **md5**

CLI (CSCF Serving-CSCF Configuration Mode)

authentication { aka-v1 *value* **| allow-auth-rsp-failure re-register | allow-hssfailure re-register | allow-noauth [invite | re-register| register] | allownoipauth [invite | re-register| register] | allow-skip-sar re-register | allow-unsecure | aor-auth | custom-md5** *value* **| md5** *value* **}**

no authentication { aka-v1 | allow-auth-rsp-failure re-register | allow-hssfailure re-register | allow-noauth [invite | re-register| register] | allownoipauth [invite | re-register| register] | allow-skip-sar re-register | allow-unsecure | aor-auth | custom-md5 | md5 }

authorization

The keyword **prov-response** has been added to this command:

CLI (CSCF Policy Rules Configuration Mode)

[default | no] authorization { early-bandwidth | prov-response }

cscf ifc-filter-criteria

The keyword **profile-part-indicator** has been made optional in this command.

CLI (Context Configuration Mode)

cscf ifc-filter-criteria id *fc_id* **priority** *pri* **[profile-part-indicator { registered | unregistered }] app-server uri scheme { sip | sips }** *as* **as-defaulthandling { session-continue | session-terminate } [-noconfirm] | [service-info** *info* **] [trigger-point** *tp_name* **] [-noconfirm] | [trigger-point** *tp_id* **] [-noconfirm]**

no cscf ifc-filter-criteria id *fc_id*

custom response

The keyword **ue-status** and its options have been added to this command. This command now configures reject with specific response code for UE capability failure or UE status.

CLI (CSCF Service Configuration Mode)

custom response { ue-capability-failure { *capability_type* **} | ue-status (** *status* **} } reject response-code {** *response_code* **}**

no custom response { ue-capability-failure { *capability_type* **} | ue-status (** *status* **} }**

deny

The following keywords and their options have been added to this command:

- **subscriber-capability**
- **user-agent**

In addition, keywords can now be entered multiple times within a single command to support multi-part ACL in CSCF.

CLI (CSCF ACL Configuration Mode)

deny { any | destination aor *aor* **| log { any | destination aor** *aor* **| source { address** *ip_address* **| aor** *aor* **} | subscriber-capability {** *capability_type* **} | user-agent device-type** *device_type* **} | source { address** *ip_address* **| aor** *aor* **} | subscriber-capability {** *capability_type* **} | user-agent device-type** *device_type* **+ }**

no deny { any | destination aor *aor* **| source { address** *ip_address* **| aor** *aor* **} | subscriber-capability {** *capability_type* **} | user-agent device-type** *device_type* **+ }**

diameter

The following dictionaries have been added/changed in this command:

- **gq-custom**
- **gq-standard**
- **rq-custom**
- **rx-custom01**
- **rx-custom02**
- **rx-custom03**
- **rx-custom04**
- **rx-custom05**
- **rx-rel8**
- **rx-standard**
- **tx-standard**

CLI (CSCF Proxy-CSCF Configuration Mode)

diameter policy-control { dictionary { gq-custom | gq-standard | rq-custom | rx-custom01 | rx-custom02 | rx-custom03 | rx-custom04 | rx-custom05 | rx-rel8 | rx-standard | tx-standard } | origin endpoint *endpoint_name* **|**

peer-select peer *peer_name* **[peer-realm** *realm_name* **] [secondary-peer** *peer_name* **[sec-peer-realm** *realm_name* **]] | request-timeout** *sec* **}**

media-bridging

The keyword **v6port-range** and its options have been added to this command.

CLI (CSCF Service Configuration Mode)

media-bridging [v6port-range *start_port end_port* **]**

no media-bridging

monitor-status

The following keywords and their options have been added to this command:

- **max-response-codes**
- **response-code**
- **timer**

CLI (CSCF Peer Server Monitoring Configuration Mode)

monitor-status { max-response-codes negative *max* **| [monitor-interval** *seconds* **] [monitor-message options [max-forwards** *max* **| response-timer** *seconds* **]] [monitor-response-timer** *seconds* **] | response-code { positive** *SIP_response_code* **| negative** *SIP_response_code* **} | timer [mark-out-of-service** *seconds* **] [unavailable-monitor-interval** *seconds* **] [unavailable-notification** *seconds* **] }**

no monitor-status { monitor | response-code [negative | positive] [*SIP_response_code* **] }**

permit

The following keywords and their options have been added to this command:

- **subscriber-capability**
- **user-agent**

In addition, keywords can now be entered multiple times within a single command to support multi-part ACL in CSCF.

CLI (CSCF ACL Configuration Mode)

permit { any | destination aor *aor* **| log { any | destination aor** *aor* **| source { address** *ip_address* **| aor** *aor* **} | subscriber-capability {** *capability_type* **} | user-agent device-type** *device_type* **} | source { address** *ip_address* **| aor** *aor* **} | subscriber-capability {** *capability_type* **} | user-agent device-type** *device_type* **+ }**

no permit { any | destination aor *aor* **| source { address** *ip_address* **| aor** *aor* **} | subscriber-capability {** *capability_type* **} | user-agent device-type** *device_type* **+ }**

registration

The keyword **implicit** and its options have been added to this command. This command now specifies the implicit amount of time that a registration can exist on the system.

CLI (CSCF Serving-CSCF Configuration Mode)

registration lifetime { default *sec* **|** **implicit** *sec* / **max** *sec* **|** **min** *sec* **}**

default registration lifetime

release-call-on-media-loss

The keyword **timeout** and its options have been added to this command.

CLI (CSCF Service Configuration Mode)

release-call-on-media-loss media-type audio [timeout *seconds* **]**

no release-call-on-media-loss

route

The following keywords and their options have been added to this command:

- **peer-servers-group**
- **route-list**

The following criteria have also been added:

- **nexthop-uri** *address*
- **subscriber-capability {** *capability_type* **}**
- **subscriber-ip-type { v4 | v6 }**

CLI (CSCF Routes Configuration Mode)

route { domain *name* **|** **local { icscf | pcscf | scscf } | nexthop-address** *address* **|** **peer-servers** *list_name* **|** **peer-servers-group** *group_name* **|** **route-list** *group_name* **|** **vpn** *name* **} [[mod-req-uri] base-criteria** *criteria* **[filter-criteria1** *criteria* **] [filter-criteria2** *criteria* **]] [log]**

no route { domain *name* **|** **local { icscf | pcscf | scscf } | nexthop-address** *address* **|** **peer-servers** *list_name* **|** **peer-servers-group** *group_name* **|** **route-list** *group_name* **|** **vpn** *name* **} base-criteria** *criteria* **[filtercriteria1** *criteria* **] [filter-criteria2** *criteria* **]**

sip-header

The keyword **p-cust1-prid-info** has been added to this command.

CLI (CSCF Proxy-CSCF Configuration Mode)

[no] sip-header insert { p-access-network-info | p-cust1-prid-info | p-user-database }

sip-header insert

The keyword **p-cust1-prid-info** has been added to this command.

CLI (CSCF Serving-CSCF Configuration Mode)

[no] sip-header insert { p-cust1-prid-info | p-user-database }

sip-param

The optional keyword **custom-logic** has been added to this command.

CLI (CSCF Proxy-CSCF Configuration Mode)

[no] sip-param insert integrity-protected [transparent]

timeout

The following keywords and their options have been added to this command:

- **map-slr-response**
- **sip c**

CLI (CSCF Service Configuration Mode)

timeout { hss-wait *sec* **| map-slr-response** *sec* **| no-answer** *sec* **| policy-interface** *sec* **| sip { 3gpp-d** *sec* **| 3gpp-t1** *msec* **| 3gpp-t2** *sec* **| 3gpp-t4** *sec* **| c** *sec* **| d** *sec* **| idle-tcp-connection** *msec* **[cleanup-timer** *msec* **] | invite-expiry** *sec* **| t1** *msec* **| t2** *sec* **| t4** *sec* **} }**

default timeout { hss-wait | map-slr-response | no-answer | policy-interface | sip { 3gpp-d | 3gpp-t1 | 3gpp-t2 | 3gpp-t4 | c | d | idle-tcp-connection | invite-expiry | t1 | t2 | t4 } }

update cscf

The following keywords and their options have been added to this command:

- **reauthentication-time**
- **reg-state**

This command can now be used to update and trigger NOTIFY for the subscribers based on reg-state and event. **contact** is an optional parameter; when **contact** is not specified, all the contact IDs associated with either a specified user or all users will be updated and trigger NOTIFY.

CLI (Exec Mode)

update cscf subscriber { all | username *user_name* **} cscf-service** *service_name* **{ { [contact** *contact_address* **] reg-state { active event { refreshed | shortened } time** *seconds* **} | terminated event { deactivated | | expired | rejected | unregistered } } | reauthentication-time** *seconds* **} [verbose]**

SGSN Commands - Modified in Release 12.0

This section provides information on SGSN commands modified in Release 12.0.

apn-resolution-dns-query snaptr

This command has been moved from the SGSN Global configuration mode to the APN Profile configuration mode.

CLI (APN Profile Configuration Mode)

[remove] apn-resolve-dns-query snaptr

apn-selection-default

New keyword ‘fallback-apn’ allows definition of a dummy APN to use when default APN is not available.

CLI (APN-Remap-Table Configuration Mode)

apn-selection-default network-identifier <apn_net_id> [fallback-apn <apn_net_id> | reject-blank-apn | require-dns-fail-wildcard | require-subscription-apn] }

no apn-selection

apn-selection-default

Three new keywords have been added to support flexible new options for using default APNs in the APN selection process:

- **first-in-subscription** - option instructs the SGSN to use the APN in the first subscription record as a default APN.
- **fallback-to-first-in-subscription** - option instructs the SGSN to use the APN in the first subscription record when configured default APN is not available.
- **prefer-single-subscription** - option instructs the SGSN to use the APN in subscription record if it is the only record available and normal APN selection fails.

CLI (APN-Remap-Table Configuration Mode)

apn-selection-default { first-in-subscription | network-identifier <> [fallback-apn network-identifier <> | fallback-to-first-in-subscription | prefer-single-subscription | reject-blank-apn | require-dns-fail-wildcard | require-subscription-apn] }

no apn-selection

authenticate

New keywords enable/disable authentication for the SMS procedure.

CLI (Call-Control Profile Configuration Mode)

authenticate sms [sms-type (mo-sms | mt-sms }] [frequency *<frequency>* **| access-type { umts | gprs }]**

no authenticate sms [sms-type (mo-sms | mt-sms }] {access-type [umts | gprs] }

default authenticate sms [sms-type (mo-sms | mt-sms }] {access-type [umts | gprs] }

authenticate

A new keyword, **on-first-vector,** instructs the SGSN to begin the MS authentication process immediately after receiving the first vector from the HLR.

CLI (Call-Control Profile Configuration Mode)

authenticate on-first-vector

remove authenticate on-first-vector

bssgp-timer

The range of the BSSGP MS flow control timer ‘th’ has been expanded (per TS 48.018) to 6 to 5999 seconds:

CLI (SGSN-Global Configuration Mode)

bssgp-timer th *<6 to 5999>*

default bssgp-timer th

cc

New keyword (**new-ni**) enables APN remapping only when the charging characteristic value in the subscription record, associated with the requested APN, matches the values configured.

CLI (GPRS Service Configuration Mode)

cc behavior *<beh_val>* **profile** *<prof_val>* **apn-remap network-identifier** *<apn_net_id>* **new-ni** *<new_apn_net_id>*

no cc behavior *<beh_val>* **profile** *<prof_val>* **apn-remap network-identifier** *<apn_net_id>*

ciphering algorithm

New keywords - **negotiation-failure-action** - have been added to configure the SGSN's action if there is not a match between the MS and SGSN ciphering algorithm configurations. As well, the call Attach/RAU Rejection message may include a configurable GMM failure code.

CLI (GPRS Service Configuration Mode)

ciphering-algorithm { negotiation-failure-action { reject [failure-code] | use-geo0 } | priority *priority* **}**

default ciphering-algorithm negotiation-failure-action

dns-extn

New keyword in the command enables the SGSN to append geographical information to the APN string that is being sent in the DNS query.

CLI (APN-Profile Configuration Mode)

dns-extn { lac-rac | msisdn start-offset <*start_digits***> end-offset** *<end_digits>*

dns-extn

If the DNS is configured to support, then inclusion of two new keywords - charg-id and rnc-id - facilitate GGSN selection.

CLI (APN-Profile Configuration Mode)

dns-extn { charg-id { binary | decimal | hexadecimal } | lac-rac | msisdn | rnc-id [charg-id { binary | decimal | hexadecimal }] }

remove dns-extn { charg-id | rnc-id [charg-id] }

gateway-address

New keyword assigns GGSN to a secondary pool of GGSNs.

CLI (APN-Profile Configuration Mode)

gateway-address *<IPv4 or IPv6>* **weight** *<1-100>* **secondary-pool**

gmm

New keywords enable validation of P-TMSI signature in the Attach Request against the P-TMSI signature stored at the SGSN. As well, optionally a GMM reject cause code can be configured.

CLI (GPRS Service Configuration Mode)

gmm attach ptmsi-signature-mismatch send-reject [failure-code *<2...111>* **]**

default gmm attach ptmsi-signature-mismatch

gmm

The CLI range for the parameter “gmm implicit-detach-timeout” is enhanced. The default value has not been changed.

CLI (SGSN Service Configuration Mode)

gmm implicit-detach-timeout < 1..86400 >

gtpc

Configures the diffserv code point marking to be used when sending GTP-C messages originating from the session manager and SGTPC manager.

CLI (SGTP Service Configuration Mode)

gtpc ip qos-dscp { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | ef }

default gtpc ip qos-dscp

gtpc

Inclusion of this new keyword, target-identification-preamble, allows the SGSN to ignore the default behavior and enables the SGSN to send the preamble byte in the Target Identification IE in the Relocation Request message:

CLI (SGTP Service Configuration Mode)

[default | no] gtpc send target-identification-preamble

gtpp dictionary

The custom33 keyword has been enabled to allow inclusion of the custom33 dictionary in the billing context configuration and to associate the dictionary with the GTPP server group for the billing context.

CLI (Context Configuration Mode)

gtpp dictionary custom33

CLI (GTPP Server Group Configuration Mode)

gtpp dictionary custom33

gtpp storage-server local file

New keyword "file-name-pattern" defines a pattern for the file name that will be used to match against the files to be purged.

CLI (GTPP Server Group Configuration Mode)

gtpp storage-server local file purge-processed-files file-name-pattern <*name_pattern*>

gtp send

The **rai** keyword has been added to configure the SGSN to include the RAI of the SGSN in CPCQ and UPCQ messages to the GGSN.

CLI (GTPP Server Group Configuration Mode)

gtp send { imeisv | ms-timezone | rai | rat | uli }

[no | remove] gtp send rai

gtp send rai

New CLI configuration options are provided in the Call Control Profile Configuration Mode for the command gtp send rai to choose PLMN value in RAI if 3G network-sharing is enabled:

- **use-local-plmn**: This keyword includes the local PLMN when network is not shared.
- **network-sharing**: This keyword is used to configure network-sharing.
- **use-selected-plmn**: This keyword includes the Selected PLMN when network is shared.
- **use-ue-plmn** : This keyword includes Selected PLMN for supporting UE and Common PLMN for non-supporting UE when network is shared.
- **use-common-plmn**: This keyword includes the Common PLMN when network is shared.

CLI (Call Control Profile Configuration Mode)

gtp send rai [use-local-plmn [network-sharing {use-selected-plmn | use-ue-plmn | use-common-plmn}]]

gtp send uli

New CLI configuration options are provided in the Call Control Profile Configuration Mode for the command gtp send uli to choose PLMN value in ULI if 3G network-sharing is enabled:

- **use-local-plmn**: This keyword includes the local PLMN when network is not shared.
- **network-sharing**: This keyword is used to configure network-sharing.
- **use-selected-plmn**: This keyword includes the Selected PLMN when network is shared.
- **use-ue-plmn** : This keyword includes Selected PLMN for supporting UE and Common PLMN for non-supporting UE when network is shared.

use-common-plmn: This keyword includes the Common PLMN when network is shared.

CLI (Call Control Profile Configuration Mode)

```
gtp send uli [use-local-plmn [network-sharing {use-selected-plmn |
use-ue-plmn | use-common-plmn}]]
```

hop-count

The configurable number of hop counts for an SCCP network instance has been expanded to 15.

CLI (SCCP-Network Configuration Mode)

```
hop-count <1-15>
```

imsi-range

The **description** keyword has been added to the IMSI range configuration to clarify use of the ranges when Release 9.0 Operator Policy configurations are converted for use with the Operator Policy functionality of Release 12.0.

CLI (SGSN-Global Configuration Mode)

```
imsi-range mcc <mcc> mnc <mnc> msin first <msin> last <msin>
operator-policy <policy_name> description <description>
```

iu-hold-connection

The range of the parameter “iu-hold-connection” is modified, the minimum permissible limit is changed from “10” seconds to “1” second.

IMPORTANT

It is recommended to use a minimum value of “10” seconds. If a value less than “10” seconds is used, more collisions may be observed. If the minimum value of “1” is set, after a re-load, INTRA-RAU (with unknown ptmsi, old-rai known) will be released in “1” second if the Identity Rsp does not come within “1” second.

CLI (IuPS Service Configuration Mode)

```
iu-hold-connection always hold-time <1..3600>
iu-hold-connection requested-by-ms hold-time <1..3600>
```

llc

A new **random-value-in-iov-ui** keyword in the **llc** command enables the SGSN to send random IOV-UI values, in XID messages, rather than the default value of zero.

CLI (GPRS-Service Configuration Mode)

```
[ default | no ] llc random-value-in-iov-ui
```

link-aggregation redundancy

New keywords enable the operator to provision port link aggregation across multiple side-by-side XGLCs -- horizontal link aggregation.

CLI (Port Ethernet Configuration Mode)

link-aggregation redundancy { standard | switched } [hold-time *<seconds>* **]**
[preferred slot { none | *<slot#>* **}]**

link id <id> link-type { highspeed-narrowband | lowspeed-narrowband }

Ranges and defaults for various MTP2 timers have been modified for ANSI and ITU variants for both SS7 lowspeed-narrowband and SS7 highspeed-narrowband links.

CLI (Link Configuration Mode)

Low-speed, ITU and ANSI; new defaults below:

- **mtp2-tmr-t1** - ITU default value is 40s and ANSI default value is 13s
- **mtp2-tmr-t2** - ITU default value is 5s, ANSI default value is 11.5s
- **mtp2-tmr-t3** - ITU default value is 1.5s, ANSI default value is 11.5s
- **mtp2-tmr-t4e** - ITU default value is 500ms, ANSI default value is 600ms
- **mtp2-tmr-t4n** - ITU default value is 8.2s, ANSI default value is 2.3s

Low-speed, ITU and ANSI; new ranges below:

- **mtp2-tmr-t1** - ITU & ANSI ranges are 120 - 500
- **mtp2-tmr-t3** - ITU & ANSI ranges are 10 - 140
- **mtp2-tmr-t4n** - ITU & ANSI ranges are 20 - 95
- **mtp2-tmr-t6** - ITU & ANSI ranges are 10 - 60

High-speed, ITU and ANSI; new defaults below:

- **mtp2-tmr-t1** - ITU default value is 300s and ANSI default value is 170s
- **mtp2-tmr-t2** - ITU default value is 5s, ANSI default value is 23s
- **mtp2-tmr-t3** - ITU default value is 1.5s, ANSI default value is 11.5s
- **mtp2-tmr-t4e** - ITU default value is 500ms, ANSI default value is 5s

Highs-peed, ITU and ANSI; new ranges below:

- **mtp2-tmr-t1** - ITU & ANSI ranges are 160 - 3500
- **mtp2-tmr-t2** - ITU & ANSI ranges are 50 - 1500
- **mtp2-tmr-t3** - ITU & ANSI ranges are 10 - 140
- **mtp2-tmr-t4e** - ITU & ANSI ranges are 4 - 60
- **mtp2-tmr-t6** - ITU & ANSI ranges are 10 - 60

mtp3-msg-size

The default number (272) of outstanding packets sent by the linkmgr (MTP2), for both high-speed and low-speed narrowband SS7 links, has been changed

CLI (Link Configuration Mode)

mtp3-msg-size *<1-272>*

default mtp3-msg-size

network-initiated-pdp-activation

In support of NRPCA, new keywords identify a predefined location area code list and define a GTPP failure cause code for inclusion in activation Reject messages.

CLI (Call-Control Profile Configuration Mode)

```
network-initiated-pdp-activation { allow { primary | secondary } | restrict
{ primary | secondary } } access type { gprs | umts } { all |
location-area-list instance <instance> } failure-code <code>
```

network-sharing cs-ps-coordination

The following command has been moved from the SGSN-Service configuration mode to the IuPS-Service configuration mode:

CLI (IuPS-Service Configuration Mode)

```
[ default | no ] network-sharing cs-ps-coordination
```

network-overload-protection

New **queue-size** and **wait-time** keywords define the queue size for buffering and message age-out wait-time for optimized network overload protection.

CLI (Global Configuration Mode)

```
network-overload-protection sgsn-new-connections-per-second
#_new_connections action { drop | reject with cause { congestion | network
failure } } [ queue-size <queue_size> ] [ wait-time <wait_time> ]
```

```
default network-overload-protection
```

pdp-deactivation-rate

The lowest values of the configurable ranges have been decreased from 20 to 1 for the rate at which the SGSN deactivates PDP for both the connected-ready and idle-standby subscriber connections. The rate is per second per SessMgr when GPT-C path failure is detected.

CLI (SGSN-Global Configuration Mode)

```
pdp-deactivation-rate { connected-ready <1-1000> | idle-standby <1-1000> }
```

qos class

New **mbr-map-down** and **mbr-map-up** keywords enable override mapping to replace a maximum bit rate (MBR) received from the HLR with locally configured MBR.

CLI (APN-Profile Configuration Mode)

```
qos class { background | conversational | interactive | streaming } [
mbr-map-down from from_kbps to to_kbps | mbr-map-up from from_kbps to
to_kbps ]
```

qos class

The following keywords have been removed from the command:

- **default**
- **no**

The following keywords have been added to the command:

- **all-values**
- **arp**
- **mbr-map-down**
- **mbr-map-up**
- **thp**
- **remove**

CLI (APN-Profile Configuration Mode)

[remove] qos class { background | conversational | interactive | streaming } [all-values | arp | gbr-down | gbr-up | mbr-down | mbr-map-down | mbr-map-up | mbr-up | min-transfer-delay | residual-bit-error-rate | sdu | thp]

ranap global-cn-id

A new keyword enables the SGSN to use a 'selected-plmn' in the plmn-part of the Global Core Network ID IE in Reset/Ack and Reset-Resource/Ack messages when network sharing has been enabled.

CLI (IuPS Service Configuration Mode)

ranap global-cn-id { reset-procedure | reset-resource-procedure } [network-sharing selected-plmn]

[default | no] ranap global-cn-id { reset-procedure | reset-resource-procedure }

release-compliance

This command has been modified to allow the operator to configure QoS overrides for both pre-release 7 and release 7 compliant RNC. New keywords are **gbr-down, gbr-up, mbr-down,** and **mbr-up**.

CLI (RNC Configuration Mode)

release-compliance { pre-release-7 | release-7 } [gbr-down <*gbr_dn_val***> | gbr-up <***gbr_up_val***> | mbr-down <***mbr_dn_val***> | mbr-up <***mbr_up_val***>] +**

default release-compliance

sctp-rto-min / sctp-sack-period

Include this keyword with the following commands in the PSP configuration mode. Enter it before entering a value. This enables configuration with finer granuality - in 10 millisecond units.

CLI (PSP Configuration Mode)

sctp-rto-min units-10ms *<1-500>*

sctp-sack-period units-10ms *<1-500>*

sgsn offload

Enable targeting an SGSN for offloading.

CLI (Exec Mode)

```
sgsn offload [ gprs-service <srvc_name> | sgsn-service <srvc_name> } {
activating | connecting [ nri-value <nri_value> | stop [ target-nri
<target_nri> target-count <target_count> ] | t3312-timeout <seconds> [
target-nri <target_nri> target-count <target_count> ] | target-nri
<target_nri> target-count <target_count> }
```

show linecard

A new keyword has been added to display new DLCI-Util statistics.

CLI (Bulkstat Configuration Mode)

```
show linecard { dlci-utilization | table }
```

show variables

A new keyword has been added to display the variables in the new DLCI-Util schema.

CLI (Bulkstat Configuration Mode)

```
show variables dlci-util
```

service timers changed

Four timers have had changes to their ranges and two timers have had changes to their defaults:

CLI (IuPS Service Configuration Mode)

- **reset ack-timeout** range has been expanded from 5 - 10 to 5 - 60 seconds. Default has increased to 20 seconds.
- **reset guard-timeout** range has been expanded from 5 - 10 to 5 - 60 seconds.
- **tigoc-timeout** range has been expanded from 1 - 10 to 1 - 60 seconds
- **tintc-timeout** range has been expanded from 1 - 10 to 1 - 60 seconds and the default has been increased to 30 seconds.

sndcp reassembly-timeout

The default (now 30 seconds) and maximum range of seconds (now 1 to 300) configurable for the SNDCP reassembly timer have been changed to facilitate support for the reordering of sub-network dependent convergence protocol N-PDU segments that arrive out-of-order.

CLI (GPRS Service Configuration Mode)

```
sndcp reassembly-timeout <seconds>
```

```
default sndcp reassembly-timeout
```

SGSN Commands - Modified in Release 12.1

This section provides information on SGSN commands modified in Release 12.1.

apn-selection-default

New keyword ‘fallback-apn’ allows definition of a dummy APN to use when default APN is not available.

CLI (APN-Remap-Table Configuration Mode)

apn-selection-default network-identifier *<apn_net_id>* **[fallback-apn** *<apn_net_id>* **| reject-blank-apn | require-dns-fail-wildcard | require-subscription-apn] }**

no apn-selection

apn-selection-default

Three new keywords have been added to support flexible new options for using default APNs in the APN selection process:

- **first-in-subscription** - option instructs the SGSN to use the APN in the first subscription record as a default APN.
- **fallback-to-first-in-subscription** - option instructs the SGSN to use the APN in the first subscription record when configured default APN is not available.
- **prefer-single-subscription** - option instructs the SGSN to use the APN in subscription record if it is the only record available and normal APN selection fails.

CLI (APN-Remap-Table Configuration Mode)

apn-selection-default { first-in-subscription | network-identifier *<net_id>* **[fallback-apn network-identifier** *<net_id>* **| fallback-to-first-in-subscription | prefer-single-subscription | reject-blank-apn | require-dns-fail-wildcard | require-subscription-apn] }**

no apn-selection

authenticate

New keywords enable/disable authentication for the SMS procedure.

CLI (Call-Control Profile Configuration Mode)

authenticate sms [sms-type (mo-sms | mt-sms }] [frequency *<frequency>* **| access-type { umts | gprs }]**

no authenticate sms [sms-type (mo-sms | mt-sms }] {access-type [umts | gprs] }

default authenticate sms [sms-type (mo-sms | mt-sms }] {access-type [umts | gprs] }

bssgp-timer

The range of the BSSGP MS flow control timer ‘th’ has been expanded (per TS 48.018) to 6 to 5999 seconds:

CLI (SGSN-Global Configuration Mode)

bssgp-timer th *<6 to 5999>*

default bssgp-timer th

ciphering algorithm

New keywords - **negotiation-failure-action** - have been added to configure the SGSN's action if there is not a match between the MS and SGSN ciphering algorithm configurations. As well, the call Attach/RAU Rejection message may include a configurable GMM failure code.

CLI (GPRS Service Configuration Mode)

ciphering-algorithm { negotiation-failure-action { reject [failure-code <*code*>] | use-geo0 } | priority <*priority*> }

default ciphering-algorithm negotiation-failure-action

dns-extn

New keyword in the command enables the SGSN to append geographical information to the APN string that is being sent in the DNS query.

CLI (APN-Profile Configuration Mode)

dns-extn { lac-rac | msisdn start-offset *<start_digits>* **end-offset** *<end_digits>*

gateway-address

New keyword assigns GGSN to a secondary pool of GGSNs.

CLI (APN-Profile Configuration Mode)

gateway-address *<IPv4 or IPv6>* **weight** *<1-100>* **secondary-pool**

gtpc

Configures the diffserv code point marking to be used when sending GTP-C messages originating from the session manager and SGTPC manager.

CLI (SGTP Service Configuration Mode)

gtpc ip qos-dscp { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | ef }

default gtpc ip qos-dscp

gtpc

Inclusion of this new keyword, target-identification-preamble, allows the SGSN to ignore the default behavior and enables the SGSN to send the preamble byte in the Target Identification IE in the Relocation Request message:

CLI (SGTP Service Configuration Mode)

[default | no] gtpc send target-identification-preamble

gtpp dictionary

The custom33 keyword has been enabled to allow inclusion of the custom33 dictionary in the billing context configuration and to associate the dictionary with the GTPP server group for the billing context.

CLI (Context Configuration Mode)

gtpp dictionary custom33

CLI (GTPP Server Group Configuration Mode)

gtpp dictionary custom33

gtpp storage-server local file

New keyword "file-name-pattern" defines a pattern for the file name that will be used to match against the files to be purged.

CLI (GTPP Server Group Configuration Mode)

gtpp storage-server local file purge-processed-files file-name-pattern <*name_pattern*>

gtp send

The **rai** keyword has been added to configure the SGSN to include the RAI of the SGSN in CPCQ and UPCQ messages to the GGSN.

CLI (GTPP Server Group Configuration Mode)

gtp send { imeisv | ms-timezone | rai | rat | uli }

[no | remove] gtp send rai

hop-count

The configurable number of hop counts for an SCCP network instance has been expanded to 15.

CLI (SCCP-Network Configuration Mode)

hop-count *<1-15>*

imsi-range

The **description** keyword has been added to the IMSI range configuration to clarify use of the ranges when Release 9.0 Operator Policy configurations are converted for use with the Operator Policy functionality of Release 12.0.

CLI (SGSN-Global Configuration Mode)

imsi-range mcc <*mcc*> mnc <*mnc*> msin first <*msin*> last <*msin*> operator-policy <*policy_name*> description <*description*>

link-aggregation redundancy

New keywords enable the operator to provision port link aggregation across multiple side-by-side XGLCs -- horizontal link aggregation.

CLI (Port Ethernet Configuration Mode)

link-aggregation redundancy { standard | switched } [hold-time *<seconds>* **] [preferred slot { none |** *<slot#>* **}]**

link id <id> link-type { highspeed-narrowband | lowspeed-narrowband }

Ranges and defaults for various MTP2 timers have been modified for ANSI and ITU variants for both SS7 lowspeed-narrowband and SS7 highspeed-narrowband links.

CLI (Link Configuration Mode)

Low-speed, ITU and ANSI; new defaults below:

- **mtp2-tmr-t1** - ITU default value is 40s and ANSI default value is 13s

- **mtp2-tmr-t2** - ITU default value is 5s, ANSI default value is 11.5s
- **mtp2-tmr-t3** - ITU default value is 1.5s, ANSI default value is 11.5s
- **mtp2-tmr-t4e** - ITU default value is 500ms, ANSI default value is 600ms
- **mtp2-tmr-t4n** - ITU default value is 8.2s, ANSI default value is 2.3s

Low-speed, ITU and ANSI; new ranges below:

- **mtp2-tmr-t1** - ITU & ANSI ranges are 120 - 500
- **mtp2-tmr-t3** - ITU & ANSI ranges are 10 - 140
- **mtp2-tmr-t4n** - ITU & ANSI ranges are 20 - 95
- **mtp2-tmr-t6** - ITU & ANSI ranges are 10 - 60

High-speed, ITU and ANSI; new defaults below:

- **mtp2-tmr-t1** - ITU default value is 300s and ANSI default value is 170s
- **mtp2-tmr-t2** - ITU default value is 5s, ANSI default value is 23s
- **mtp2-tmr-t3** - ITU default value is 1.5s, ANSI default value is 11.5s
- **mtp2-tmr-t4e** - ITU default value is 500ms, ANSI default value is 5s

High-speed, ITU and ANSI; new ranges below:

- **mtp2-tmr-t1** - ITU & ANSI ranges are 160 - 3500
- **mtp2-tmr-t2** - ITU & ANSI ranges are 50 - 1500
- **mtp2-tmr-t3** - ITU & ANSI ranges are 10 - 140
- **mtp2-tmr-t4e** - ITU & ANSI ranges are 4 - 60
- **mtp2-tmr-t6** - ITU & ANSI ranges are 10 - 60

network-initiated-pdp-activation

In support of NRPCA, new keywords identify a predefined location area code list and define a GTPP failure cause code for inclusion in activation Reject messages.

CLI (Call-Control Profile Configuration Mode)

```
network-initiated-pdp-activation { allow { primary | secondary } | restrict
{ primary | secondary } } access type { gprs | umts } { all |
location-area-list instance <instance> } failure-code <code>
```

pdp-deactivation-rate

The lowest values of the configurable ranges have been decreased from 20 to 1 for the rate at which the SGSN deactivates PDP for both the connected-ready and idle-standby subscriber connections. The rate is per second per SessMgr when GPT-C path failure is detected.

CLI (SGSN-Global Configuration Mode)

```
pdp-deactivation-rate { connected-ready <1-1000> | idle-standby <1-1000> }
```

qos class

New **mbr-map-down** and **mbr-map-up** keywords enable override mapping to replace a maximum bit rate (MBR) received from the HLR with locally configured MBR.

CLI (APN-Profile Configuration Mode)

qos class { background | conversational | interactive | streaming } [mbr-map-down from *<from_kbps>* **to** *<to_kbps>* **| mbr-map-up from** *<from_kbps>* **to** *<to_kbps>* **]**

qos class

The following keywords have been removed from the command:

- **default**
- **no**

The following keywords have been added to the command:

- **all-values**
- **arp**
- **mbr-map-down**
- **mbr-map-up**
- **thp**
- **remove**

CLI (APN-Profile Configuration Mode)

[remove] qos class { background | conversational | interactive | streaming } [all-values | arp | gbr-down | gbr-up | mbr-down | mbr-map-down | mbr-map-up | mbr-up | min-transfer-delay | residual-bit-error-rate | sdu | thp]

ranap global-cn-id

A new keyword enables the SGSN to use a ‘selected-plmn’ in the plmn-part of the Global Core Network ID IE in Reset/Ack and Reset-Resource/Ack messages when network sharing has been enabled.

CLI (IuPS Service Configuration Mode)

ranap global-cn-id { reset-procedure | reset-resource-procedure } [network-sharing selected-plmn]

[default | no] ranap global-cn-id { reset-procedure | reset-resource-procedure }

sctp-rto-min / sctp-sack-period

Include this keyword with the following commands in the PSP configuration mode. Enter it before entering a value. This enables configuration with finer granuality - in 10 millisecond units.

CLI (PSP Configuration Mode)

sctp-rto-min units-10ms *<1-500>*

sctp-sack-period units-10ms *<1-500>*

sgsn offload

Enable targeting an SGSN for offloading.

CLI (Exec Mode)

sgsn offload [gprs-service *<srvc_name>* **| sgsn-service** *<srvc_name>* **} {**
activating | connecting [nri-value *<nri_value>* **| stop [target-nri**
<target_nri> **target-count** *<target_count>* **] | t3312-timeout** *<seconds>* **[**
target-nri *<target_nri>* **target-count** *<target_count>* **] | target-nri**
<target_nri> **target-count** *<target_count>* **}**

service timers changed

Four timers have had changes to their ranges and two timers have had changes to their defaults:

CLI (IuPS Service Configuration Mode)

- **reset ack-timeout** range has been expanded from 5 - 10 to 5 - 60 seconds. Default has increased to 20 seconds.
- **reset guard-timeout** range has been expanded from 5 - 10 to 5 - 60 seconds.
- **tigoc-timeout** range has been expanded from 1 - 10 to 1 - 60 seconds
- **tintc-timeout** range has been expanded from 1 - 10 to 1 - 60 seconds and the default has been increased to 30 seconds.

sndcp reassembly-timeout

The default (now 30 seconds) and maximum range of seconds (now 1 to 300) configurable for the SNDCP reassembly timer have been changed to facilitate support for the reordering of sub-network dependent convergence protocol N-PDU segments that arrive out-of-order.

CLI (GPRS Service Configuration Mode)

sndcp reassembly-timeout *<seconds>*

default sndcp reassembly-timeout

SGSN Commands - Modified in Release 12.2

This section provides information on SGSN commands modified in Release 12.2.

action

The range for the number of actions configurable per GTT association has been increased from 8 to 15.

CLI (GTPP Server Group Configuration Mode)

action id *<id>* **type** *<action_type>* **start-digit** *<value>* **end-digit** *<value>*

no action id *<id>*

authenticate

A new keyword, **on-first-vector,** instructs the SGSN to begin the MS authentication process immediately after receiving the first vector from the HLR.

CLI (Call-Control Profile Configuration Mode)

authenticate on-first-vector

remove authenticate on-first-vector

authenticate

The authenticate command has been re-architected to provide interface consistency and to allow the operator to enable the functions as needed. The function of the 'no' keyword in all instances now disables the specified function. Several new keywords have been added; see the *Command Line Interface Reference* for use and function information for all of these new keywords:

- **attach-type { combined | gprs-only }**
- **foreign-ptmsi**
- **frequency**
- **local-ptmsi**
- **periodicity**
- **remove**

This function is no longer enabled by default, so the **default** keyword has been removed (deprecated).

CLI (Call Control Profile Configuration Mode)

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 }]]

authenticate all-events [access-type { gprs | umts } | frequency <*frequency*> [access-type { gprs | umts }]]

[no | remove] authenticate all-events [access-type { gprs | umts }]

authenticate attach [access-type { gprs | umts } | attach-type { combined | gprs-only } | frequency <*frequency*> | inter-rat] [access-type { gprs | umts }]

[no | remove] authenticate attach [access-type { gprs | umts } | attach-type { combined | gprs-only } | inter-rat] [access-type { gprs | umts }]

authenticate detach access-type { gprs | umts }

[no | remove] authenticate detach [access-type { gprs | umts }

authenticate rau [access-type { gprs | umts } | frequency <*frequency*> | periodicity <*duration*> | update-type { combined-update | imsi-combined-update | periodic | ra-update [with { foreign-ptmsi |

inter-rat-local-ptmsi | local-ptmsi }]] [access-type { gprs | umts } | frequency <*frequency*> **| periodicity** <*duration*> **]**

no authenticate rau [access-type { grps | umts } | update-type { combined-update | imsi-combined-update | periodic | ra-update [with { foreign-ptmsi | inter-rat-local-ptmsi | local-ptmsi } [access-type { gprs | umts }]

remove authenticate rau [access-type { gprs | umts } | periodicity | update-type { combined-update | imsi-combined-update | periodic | ra-update [periodicity | with { foreign-ptmsi | inter-rat-local-ptmsi | local-ptmsi } [access-type { gprs | umts }]

authenticate service-request [frequency <*frequency*> **| periodicity** <*duration*> **| service-type { data | page-response | signaling } [frequency** <*frequency*> **| periodicity** <*duration*> **]]**

no authenticate service-request [service-type { data | page-response | signaling }]

remove authenticate service-request [periodicity | service-type { data | page-response | signaling } [periodicity]]

authenticate sms [access-type { gprs | umts } | frequency <*frequency*> **| sms-type { mo-sms | mt-sms }] [access-type { gprs | umts } | frequency** <*frequency*> **]**

[no | remove] authenticate sms [access-type { gprs | umts } | sms-type { mo-sms | mt-sms } [access-type { gprs umts }]]

cc

New keyword (**new-ni**) enables APN remapping only when the charging characteristic value in the subscription record, associated with the requested APN, matches the values configured.

CLI (GPRS Service Configuration Mode)

cc behavior *<beh_val>* **profile** *<prof_val>* **apn-remap network-identifier** *<apn_net_id>* **new-ni** *<new_apn_net_id>*

no cc behavior *<beh_val>* **profile** *<prof_val>* **apn-remap network-identifier** *<apn_net_id>*

gmm

New keywords enable validation of P-TMSI signature in the Attach Request against the P-TMSI signature stored at the SGSN. As well, optionally a GMM reject cause code can be configured.

CLI (GPRS Service Configuration Mode)

gmm attach ptmsi-signature-mismatch send-reject [failure-code *<2...111>* **]**

default gmm attach ptmsi-signature-mismatch

gtpp attribute

In support of IPv4v6 dual PDP address types, this new keyword enables the SGSN to include IPv4v6 address information in the S-CDR. The IPv4 address goes in the new PDP address extension field and the IPv6 address goes in the existing servedPDPAddress field.

CLI (GTPP Server Group Configuration Mode)

[default | no] gtpp attribute served-pdp-pdn-address-extension

gtpp storage-server local file

One new keyword enables (disabled by default) the use of continuous file sequence numbers and the second new keyword allows for recovery of file sequence numbers in the event of aaaproxy or chassis restarts/reboots.

CLI (GTPP Server Group Configuration Mode)

gtpp storage-server local file { compression | format | name | purge-processed-files | rotation | start-file-seq-num <*number*> [recover-file-seq-num] }

default gtpp storage-server local file start-file-seq-num

logging filter

New **gtpu** and **gtpumgr** logging filters enable the creation of Debug Logs specific to the GTPU information for the peer RNCs/GGSNs.

CLI (Exec Mode

[no] logging filter active facility [gtpu | gtpumgr] level [critical | error | warning | unusual | info | trace | debug]

network-sharing cs-ps-coordination

The following command has been moved from the SGSN-Service configuration mode to the IuPS-Service configuration mode:

CLI (IuPS-Service Configuration Mode)

[default | no] network-sharing cs-ps-coordination

ptmsi-reallocate

The range of values has been expanded for the **interval** parameter:

CLI (Call Control Profile Configuration Mode)

ptmsi-reallocate interval *<1 - 1440>*

ptmsi-reallocate

The **remove** keyword has been added to delete P-TMSI reallocation definitions from the configuration file. This function is no longer enabled by default, so the **default** keyword has been removed (deprecated).

CLI (Call Control Profile Configuration Mode)

[no | remove] ptmsi-reallocate { attach | frequency | interval | routing-area-update [update-type { combined-update | imsi-combined-update | periodic | ra-update }] | service-request [service-type { data | page-response | signaling }] } [access-type { gprs | umts }]

ptmsi-signature-reallocate

The range of values has been expanded for the **interval** parameter:

CLI (Call Control Profile Configuration Mode)

ptmsi-signature-reallocate interval *<1 - 1440>*

ptmsi-signature-reallocate

The **remove** keyword has been added to delete P-TMSI signature reallocation definitions from the configuration file. This function is no longer enabled by default, so the **default** keyword has been removed (deprecated).

CLI (Call Control Profile Configuration Mode)

[no | remove] ptmsi-signature-reallocate { attach | frequency | interval | routing-area-update [update-type { combined-update | imsi-combined-update | periodic | ra-update }] } [access-type { gprs | umts }]

sgsn op

New keyword displays authentication and P-TMSI reallocate and P-TMSI signature reallocate information in a new display table.

CLI (Exec Mode)

sgsn op auth-ptmsi-counters imsi *<imsi>*

show linecard

A new keyword has been added to display new DLCI-Util statistics.

CLI (Bulkstat Configuration Mode)

show linecard { dlci-utilization | table }

show iups-service

A new keyword **gtpu-table** filter allows the operator to display a table specific to GTPU information for the peer RNCs/GGSNs for the specified IuPS service.

CLI (IuPS Service Configuration Mode)

show iups-service { all | name *<srvc_name>* **} [gtpu-table | rnc { all | id** *<rnc_id>* **}] [| { grep** *<grep_options>* **| more }]**

show sgtp-service

A new keyword **gtpu-table** filter allows the operator to display a table specific to GTPU information for the peer RNCs/GGSNs for the specified SGTP service.

CLI (SGTP Service Configuration Mode)

show sgtp-service { all [gtpu-table] | ggsn-table [smgr-instance *<smgr_instance>* **] | mbms-bearers | name** *<srvc_name>* **[gtpu-table] | sgsn-table }**

show variables

A new keyword has been added to display the variables in the new DLCI-Util schema.

CLI (Bulkstat Configuration Mode)

show variables dlci-util

wildcard-apn pdp-type

New keyword allows the operator to configure a wildcard subscription with PDP type IPv4v6 for an SGSN default APN.

CLI (APN Remap Table Configuration Mode)

wildcard-apn pdp-type { dual-ipv4v6 | ipv4 | ipv6 | ppp } network-identifier *<apn_net_id>*

no wildcard-apn pdp-type dual-ipv4v6

TPO Commands Modified in Release 12.0

This section provides information on TPO commands modified in release 12.0.

tcp fast-retransmit-dupacks

This command specifies the number of duplicate ACKs required for fast retransmission. The **dynamic** keyword was added to this command. This enables to dynamically change the number of duplicate ACKs required for fast retransmission based on the number of in-flight packets (one-third of the in-flight packets, subject to a minimum of two). This enables to eliminate spurious retransmissions when packet reordering in the network is high.

CLI (ACS TPO Profile Configuration Mode)

tcp fast-retransmit-dupacks { *duplicate_acks* **| dynamic }**

default tcp fast-retransmit-dupacks

TPO Commands Modified in Release 12.2

This section provides information on TPO commands modified in release 12.2.

match-rule priority

This command specifies the TPO profile to use when the traffic matches a particular TPO ruledef/TPO group-of-ruledefs. This command now enables to configure TPO group-of-ruledefs.

CLI (ACS TPO Profile Configuration Mode)

match-rule priority *rule_priority* **{ tpo-group-of-ruledefs** *tpo_group_of_ruledefs_name* **|** **tpo-ruledef** *tpo_ruledef_name* **} tpo { none |** **profile** *tpo_profile_name* **} [description** *description* **]**

no match-rule priority *rule_priority*

tcp fast-retransmit-dupacks

This command specifies the number of duplicate ACKs required for fast retransmission. In the 12.2 and later releases, the behavior of the **dynamic** keyword has changed. Now the **dynamic** keyword specifies to dynamically change the number of duplicate ACKs required for fast retransmission based on the number of in-flight packets, and controls the actions taken on D-SACK detection.

CLI (ACS TPO Profile Configuration Mode)

tcp fast-retransmit-dupacks { *duplicate_acks* **|** **dynamic }**

default tcp fast-retransmit-dupacks

Obsoleted Commands

This section identifies configuration commands that have been obsoleted in Release 12.x.

Common Commands - Obsoleted in Release 12.0

This section provides information on commands that are common to all products that were obsoleted in Release 12.0.

None for this release.

Common Commands - Obsoleted in Release 12.2

This section provides information on commands that are common to all products that were obsoleted in Release 12.2.

diameter sctp

This command has been removed from the 12.2 release and replaced with the **`associate sctp-parameters-template`** command in the Diameter Endpoint Configuration mode.

For more details on the new command, please see the *associate* command in *Common Commands - New in Release 12.2* section.

CLI (Context Configuration Mode)

`diameter sctp { hearbeat-interval` *`interval`* **`| path max-retransmissions`** *`retransmissions`* **`}`**

`default diameter sctp { heartbeat-interval | path max-retransmissions }`

Application Detection and Control Commands - Obsoleted in Release 12.0

This section provides information on new ADC commands available in Release 12.0.

None for this release.

Content Filtering Commands - Obsoleted in Release 12.0

This section provides information on CF commands that were obsoleted in Release 12.0.

None for this release.

ECS Commands - Obsoleted in Release 12.0

This section provides information on ECS commands that were obsoleted in Release 12.0.

None for this release.

Firewall Commands - Obsoleted in Release 12.0

This section provides information on Stateful Firewall commands that were obsoleted in Release 12.0.

None for this release.

GGSN Commands - Obsoleted in Release 12.0

This section provides information on GGSN commands that were obsoleted in Release 12.0.

gtpu echo interval

This command has been obsoleted in 12.0 release and now available in GTP-U service configuration mode.

CLI (GGSN Service Configuration mode))

gtpu echo-interval time_interval

no gtpu echo-interval

gtpu reorder

This command has been obsoleted in 12.0 release.

CLI (GGSN Service Configuration mode))

gtpu reorder { context { ppp } | sequence-numbers { ipv4 | ppp | ipv4-ppp | ppp-ipv4 } | timeout *time* **}**

[no] gtpu reorder { context | sequence-numbers { ipv4 | ppp | ipv4-ppp | ppp-ipv4 } }

gtpu udp-checksum insert

This command has been obsoleted in 12.0 release.

CLI (GGSN Service Configuration mode))

```
[ default | no ] gtpu udp-checksum insert
```

HA Commands - Obsoleted in Release 12.0

This section provides information on HA commands that were obsoleted in Release 12.0.

None for this release.

IPCF Commands - Obsoleted in Release 12.1

This section provides information on IPCF commands that were obsoleted in Release 12.1.

IPCF is new product for this release.

Mobility Management Entity Commands - Obsoleted in Release 12.0

This section provides information on MME commands that were obsoleted in Release 12.0.

mme-policy

This command has been removed from the 12.0 release and replaced with the **`lte-policy`** command.

CLI (Global Configuration Mode)

`mme-policy`

PDSN Commands - Obsoleted in Release 12.0

This section provides information on PDSN commands that were obsoleted in Release 12.0.

None for this release.

Session Control Manager Commands - Obsoleted in Release 12.0

This section provides information on SCM commands that were obsoleted in Release 12.0.

authorization

This command functionality has been moved to the CSCF PCRF-Policy-Control Configuration Mode and expanded.

CLI (CSCF Proxy-CSCF Configuration Mode)

`[ no ] authorization non-video`

policy

This command functionality has been moved to the CSCF Service Configuration Mode and expanded.

CLI (CSCF Policy Rules Configuration Mode)

`policy overload { redirect` *`address1`* **`[ weight`** *`weight1`* **`] [`** *`address2`* **`[ weight`** *`weight2`* **`] ] ... | reject [ use-reject-code { admin-prohibited | insufficient-resources } ] }`**

`default policy overload`

`no policy overload redirect` *`address1`* **`[`** *`address2`* **`] ...`**

subscribe

This command has been removed from the 12.0 release and replaced with the **signaling-bearer-loss** command in the CSCF PCRF-Policy-Control Configuration Mode.

CLI (CSCF Proxy-CSCF Configuration Mode)

```
[ no ] subscribe signaling-bearer-loss
```

SGSN Commands - Obsoleted in Release 12.0

This section provides information on SGSN commands that were obsoleted in Release 12.0.

check-imei-timeout-action

This command in the SGSN-Service configuration mode has been replaced by the check-imei command in both the SGSN-Service and GPRS-Service configuration modes.

gmm-sm-statistics attach-rejects

This command, in the SGSN-Global configuration mode, has been deprecated because the default behavior has been modified so that the SGSN automatically generates segregated internal and external statistics.

ignore-remote-restart-counter

This command, in the SGTP Service configuration mode, has been deprecated because the default behavior has been modified so that the SGSN verifies the remote restart counter changes observed in the PDP establishment messages and to ensure no mistaken configuration leads to genuine GGSN restarts being ignored. For information about the behavioral change, see the *New Features* section.

SGSN Commands - Obsoleted in Release 12.2

This section provides information on SGSN commands that were obsoleted in Release 12.2.

check-imei-timeout-action

This command in the SGSN-Service configuration mode has been replaced by the check-imei command in both the SGSN-Service and GPRS-Service configuration modes.

ignore-remote-restart-counter

This command, in the SGTP Service configuration mode, has been deprecated because the default behavior was modified in 12.0 release so that the SGSN verifies the remote restart counter changes observed in the PDP establishment messages and to ensure no mistaken configuration leads to genuine GGSN restarts being ignored. For information about the behavioral change, see the *SGSN in Release 12.0* section of the *New Features Summary* chapter.

GTPP Storage Server (GSS)

This section provides information on GSS changes in Release 12.0.

None for this release.

Policy Provisioning Tool Changes

Policy Provisioning Tool (PPT) support is new product in Release 12.1.

Cisco Policy Provisioning Tool (PPT) is a Web-based client-server application which provides the user (network operator) a comprehensive use case design experience. It enables the network operator to design a service plan and subscriber profile data modelling at a time with the help of use case design and configuration.

PPT is designed to simplify use case configuration by importing the relevant Policy Control Enforcement Function (PCEF) flow, rules and APN data elements.

PCEF, typically located at the gateway is responsible for enforcing the policy and charging related decisions received from IPCF. PCEF performs service data flow detection as well as gate enforcement for the data flows.

For information about the PPT, refer *Policy Provisioning Tool Installation and Administration Guide.*

Subscriber Service Controller Changes

Subscriber Service Controller (SSC) support is new product in Release 12.1.

Subscriber Service Controller (SSC) is an application that complements and extends the functionality of Intelligent Policy Control Function (IPCF).

SSC uses Subscriber Profile Repository (SPR) data store, to implement the usage control policies in a centralized manner. It also handles account details as well as session state information of the subscriber. SSC can manage the event notification function for PCC, by sending e-mails or text messages to subscribers. SSC provides storage facility for subscriber profile along with centralized management of subscriber policy and quota for your deployment.

SSC works in conjunction with IPCF, PPT and other PCC components.

For information about the SSC, refer *Subscriber Service Controller Installation and Administration Guide.*

Web Element Manager Changes in Release 12.0

This section provides information on Web Element Manager configuration changes in Release 12.0.

Active Charging Support Moved

The Active Charging Support menu has been removed from the WEM Configuration menu. ACS functionality is now available via the CLI interface in the WEM's Load Configuration feature.

Web Element Manager Path

Configuration | Save/Load Configuration | Load Configuration

New Location for PCRF Folder in WEM High Availability Installation

During WEM installation in a High Availability environment, the **pcrf** folder was placed in the *<ems_dir>/server* directory. Now, the **pcrf** folder is placed on the shared disk so that it is available to both nodes in the cluster, and can thereby obtain data from external sources and parse the data to 3GPP format.

This is done automatically by the script once the path to the shared disk has been defined as part of the installation process.

SFTP Support for Software Upgrade

Previously, configuration files were uploaded/downloaded using the FTP protocol. A pair of radio buttons has been added to the **Software Upgrade** dialog box to choose between FTP and SFTP protocols for transferring files.

Web Element Manager Path

Configuration | Software Upgrade

FTP User Doesn't Exist Message/Passwd.Ftp Failure Alarm

If the WEM server is used as primary or secondary destination, then the user defined as the FTP user in the bulkstats configuration screen must be present/created on the WEM server by the system administrator. For the message "user for FTP-ing the files from ASR5K to WEM doesn't exist" the correct action is for the Admin to configure such a user.

This is addressed in the *Troubleshooting* chapter in the *Web Element Manager Installation and Administration Guide*.

Script Server Enabled by Default

Previously the *Web Element Manager Installation and Administration Guide* stated that the Script Server was disabled by default. The Script server is enabled by default and the documentation has been changed to reflect this.

Change to High Availability Configuration

A change has been made to the *WEM High Availability Redundancy Installations* chapter in the *WEB Element Manager Installation and Administration Guide*. Previously, in the "Uninstalling WEM with VCS" section, the instructions read:

Offline the WEM Application service resource on active node:

```
$ hares -offline <wem application resource name> -sys <node1>
```

```
$ hagrp -disable <resource group name> -sys <node1>
```

This has been modified to read:

Offline the WEM Application service resource on active node:

```
$ hares -offline <wem application resource name> -sys <node1>
```

Web Element Manager Changes in Release 12.2

This section describes the Configuration changes made in Web Element Manager Release 12.2.

Script Server Enabled by Default

Previously the documentation stated that the Script Server was disabled by default. The Script server is enabled by default and the documentation has been changed to reflect this.

Change to High Availability Configuration Instructions

A change has been made to the *WEM High Availability Redundancy Installations* chapter in the *WEB Element Manager Installation and Administration Guide*. Previously, in the "Uninstalling WEM with VCS" section, the instructions read:

Offline the WEM Application service resource on active node:

```
$ hares -offline <wem application resource name> -sys <node1>
```

```
$ hagrp -disable <resource group name> -sys <node1>
```

This has been modified to read:

Offline the WEM Application service resource on active node:

```
$ hares -offline <wem application resource name> -sys <node1>
```

CHAPTER 4
ACCOUNTING MANAGEMENT

This section contains additions and changes made to the accounting-related parameters in Release 12.0, 12.1, and 12.2.

Topics covered in this chapter are:

Bulk Statistic Enhancements

This section lists bulk statistic additions and changes in Release 12.x.

For detailed information on bulk statistics refer to the *System Administration Guide* and *Statistics and Counters Reference*.

Bulk Statistic Enhancements in Release 12.0

This section lists bulk statistic additions and changes in Release 12.0.

New Bulk Statistics

Support for the following bulk statistics were added in Release 12.0.

Context Schema

- sfw-ipv6-discardpackets
- sfw-ipv6-malpackets
- sfw-icmpv6-discardpackets
- sfw-icmpv6-malpackets

Diameter Authentication Schema

- asa-rsp-rej-sent
- req-sock-write-err
- rsp-sock-write-err
- any-sock-read-err
- rem-disconnect
- loc-disconnect

DLCI-Util Schema

- card
- port
- dlci_util_path
- dlci_util_ds1e1
- dlci_util_timeslot
- dlci_util_dlci_no
- dlci_util_nsvc
- dlci_util_nse

- dlci_util_dlci_curr_rx
- dlci_util_dlci_curr_tx
- dlci_util_dlci_5min_rx
- dlci_util_dlci_5min_tx
- dlci_util_dlci_15min_rx
- dlci_util_dlci_15min_tx

ECS Schema

- h323-calls
- h323-uplk-bytes
- h323-dwnlk-bytes
- h323-uplk-pkts
- h323-dwnlk-pkts
- h323-q931-messages
- h323-h245-messages
- h323-ras-messages
- pptp-flows
- pptp-gre-flows
- pptp-uplk-bytes
- pptp-dwnlk-bytes
- pptp-uplk-pkts
- pptp-dwnlk-pkts
- pptp-inv-pkts
- pptp-unknown-pkts
- pptp-gre-uplk-bytes
- pptp-gre-dwnlk-bytes
- pptp-gre-uplk-pkts
- pptp-gre-dwnlk-pkts
- tftp-flows
- tftp-uplk-bytes
- tftp-dwnlk-bytes
- tftp-uplk-pkts
- tftp-dwnlk-pkts
- tftp-total-read-sessions
- tftp-total-write-sessions
- tftp-unsupp-req-pkts
- tftp-invalid-ctrl-pkts
- tftp-invalid-data-pkts
- tftp-data-uplk-bytes

- tftp-data-dwnlk-bytes
- tftp-data-uplk-pkts
- tftp-data-dwnlk-pkts
- p2p-skype-unclassified-uplnk-bytes — This variable replaces p2p-skype-non-audio-uplnk-bytes.
- p2p-skype-unclassified-dwlnk-bytes — This variable replaces p2p-skype-non-audio-dwlnk-bytes.
- p2p-skype-unclassified-uplnk-pkts — This variable replacesp2p-skype-non-audio-uplnk-pkts.
- p2p-skype-unclassified-dwlnk-pkts — This variable replaces p2p-skype-non-audio-dwlnk-pkts.
- p2p-msn-unclassified-uplnk-bytes — This variable replaces p2p-msn-non-audio-or-video-uplnk-bytes.
- p2p-msn-unclassified-dwlnk-bytes — This variable replaces p2p-msn-non-audio-or-video-dwlnk-bytes.
- p2p-msn-unclassified-uplnk-pkts — This variable replaces p2p-msn-non-audio-or-video-uplnk-pkts.
- p2p-msn-unclassified-dwlnk-pkts — This variable replaces p2p-msn-non-audio-or-video-dwlnk-pkts.
- p2p-yahoo-unclassified-uplnk-bytes — This variable replaces p2p-yahoo-non-audio-uplnk-bytes.
- p2p-yahoo-unclassified-dwlnk-bytes — This variable replaces p2p-yahoo-non-audio-dwlnk-bytes.
- p2p-yahoo-unclassified-uplnk-pkts — This variable replaces p2p-yahoo-non-audio-uplnk-pkts.
- p2p-yahoo-unclassified-dwlnk-pkts — This variable replaces p2p-yahoo-non-audio-dwlnk-pkts.
- p2p-oscar-unclassified-uplnk-bytes — This variable replaces p2p-oscar-non-audio-uplnk-bytes.
- p2p-oscar-unclassified-dwlnk-bytes — This variable replaces p2p-oscar-non-audio-dwlnk-bytes.
- p2p-oscar-unclassified-uplnk-pkts — This variable replaces p2p-oscar-non-audio-uplnk-pkts.
- p2p-oscar-unclassified-dwlnk-pkts — This variable replaces p2p-oscar-non-audio-dwlnk-pkts.
- p2p-gtalk-unclassified-uplnk-bytes — This variable replaces p2p-gtalk-non-audio-uplnk-bytes.
- p2p-gtalk-unclassified-dwlnk-bytes — This variable replaces p2p-gtalk-non-audio-dwlnk-bytes.
- p2p-gtalk-unclassified-uplnk-pkts — This variable replaces p2p-gtalk-non-audio-uplnk-pkts.
- p2p-gtalk-unclassified-dwlnk-pkts — This variable replaces p2p-gtalk-non-audio-dwlnk-pkts.

- p2p-oscar-video-uplnk-bytes
- p2p-oscar-video-dwlnk-bytes
- p2p-oscar-video-uplnk-pkts
- p2p-oscar-video-dwlnk-pkts
- p2p-gtalk-video-uplnk-bytes
- p2p-gtalk-video-dwlnk-bytes
- p2p-gtalk-video-uplnk-pkts
- p2p-gtalk-video-dwlnk-pkts
- p2p-yahoo-video-uplnk-bytes
- p2p-yahoo-video-dwlnk-bytes
- p2p-yahoo-video-uplnk-pkts
- p2p-yahoo-video-dwlnk-pkts
- p2p-blackberry-uplnk-bytes
- p2p-blackberry-dwlnk-bytes
- p2p-blackberry-uplnk-pkts
- p2p-blackberry-dwlnk-pkts
- p2p-gmail-uplnk-bytes
- p2p-gmail-dwlnk-bytes
- p2p-gmail-uplnk-pkts
- p2p-gmail-dwlnk-pkts
- p2p-itunes-uplnk-bytes
- p2p-itunes-dwlnk-bytes
- p2p-itunes-uplnk-pkts
- p2p-itunes-dwlnk-pkts
- p2p-myspace-uplnk-bytes
- p2p-myspace-dwlnk-bytes
- p2p-myspace-uplnk-pkts
- p2p-myspace-dwlnk-pkts
- p2p-teamviewer-uplnk-bytes
- p2p-teamviewer-dwlnk-bytes
- p2p-teamviewer-uplnk-pkts
- p2p-teamviewer-dwlnk-pkts
- p2p-twitter-uplnk-bytes
- p2p-twitter-dwlnk-bytes
- p2p-twitter-uplnk-pkts
- p2p-twitter-dwlnk-pkts
- p2p-viber-uplnk-bytes
- p2p-viber-dwlnk-bytes

- p2p-viber-uplnk-pkts
- p2p-viber-dwlnk-pkts

eGTP-C Service Schema

- csfb-sent-suspendnotf
- csfb-sent-retranssuspendnotf
- csfb-recv-suspendnotf
- csfb-recv-retranssuspendnotf
- csfb-sent-suspendack
- csfb-sent-suspendackaccept
- csfb-sent-suspendackdenied
- csfb-recv-suspendackp
- csfb-recv-suspendackaccept
- csfb-recv-suspenddenied
- csfb-sent-resumenotf
- csfb-sent-retransresumenotf
- csfb-recv-resumenotf
- csfb-recv-retransresumenotf
- csfb-sent-resumeack
- csfb-sent-resumeackaccept
- csfb-sent-resumeackdenied
- csfb-recv-resumeackp
- csfb-recv-resumeackaccept
- csfb-recv-resumedenied

SGs Schema

This is a new schema in 12.0.

- vpnname
- vpnid
- servname
- servid
- pag-req-tx
- pag-req-retx
- pag-req-rx
- pag-rej-tx
- pag-rej-retx
- pag-rej-rx
- service-req-tx
- service-req-retx
- service-req-rx

- dl-ud-tx
- dl-ud-retx
- dl-ud-rx
- ul-ud-tx
- ul-ud-retx
- ul-ud-rx
- localupd-req-tx
- localupd-req-retx
- localupd-req-rx
- localupd-accept-tx
- localupd-accept-retx
- localupd-accept-rx
- localupd-rej-tx
- localupd-rej-retx
- localupd-rej-rx
- tmsi-reloc-tx
- tmsi-reloc-retx
- tmsi-reloc-rx
- alert-req-tx
- alert-req-retx
- alert-req-rx
- alert-ack-tx
- alert-ack-retx
- alert-ack-rx
- alert-rej-tx
- alert-rej-retx
- alert-rej-rx
- ue-actind-tx
- ue-actind-retx
- ue-actind-rx
- eps-detind-tx
- eps-detind-retx
- eps-detind-rx
- eps-detack-tx
- eps-detack-retx
- eps-detack-rx
- imsi-detind-tx
- imsi-detind-retx

- imsi-detind-rx
- imsi-detack-tx
- imsi-detack-retx
- imsi-detack-rx
- reset-ind-tx
- reset-ind-retx
- reset-ind-rx
- reset-ack-tx
- reset-ack-retx
- reset-ack-rx
- mm-inforeq-tx
- mm-inforeq-retx
- mm-inforeq-rx
- rel-req-tx
- rel-req-retx
- rel-req-rx
- status-tx
- status-retx
- status-rx
- ue-unreach-tx
- ue-unreach-retx
- ue-unreach-rx
- unk-msg-tx
- unk-msg-retx
- unk-msg-rx

SGSN Schema

- redir-attach-rej-gprs-pna
- redir-attach-rej-comb-pna
- redir-peroidic-rau-pna
- redir-rau-gprs-intra-sgsn-rej-pna
- redir-rau-comb-intra-sgsn-rej-pna
- redir-rau-gprs-inter-sgsn-rej-pna
- redir-rau-comb-inter-sgsn-rej-pna
- redir-rau-gprs-inter-rat-pna
- redir-rau-comb-inter-rat-pna
- redir-rau-gprs-inter-serv-pna
- redir-rau-comb-inter-serv-pna
- redir-attach-rej-gprs-lana

- redir-attach-rej-comb-lana
- redir-peroidic-rau-lana
- redir-rau-gprs-intra-sgsn-rej-lana
- redir-rau-comb-intra-sgsn-rej-lana
- redir-rau-gprs-inter-sgsn-rej-lana
- redir-rau-comb-inter-sgsn-rej-lana
- redir-rau-gprs-inter-rat-lana
- redir-rau-comb-inter-rat-lana
- redir-rau-gprs-inter-serv-lana
- redir-rau-comb-inter-serv-lana
- redir-attach-rej-gprs-rna
- redir-attach-rej-comb-rna
- redir-peroidic-rau-rna
- redir-rau-gprs-intra-sgsn-rej-rna
- redir-rau-comb-intra-sgsn-rej-rna
- redir-rau-gprs-inter-sgsn-rej-rna
- redir-rau-comb-inter-sgsn-rej-rna
- redir-rau-gprs-inter-rat-rna
- redir-rau-comb-inter-rat-rna
- redir-rau-gprs-inter-serv-rna
- redir-rau-comb-inter-serv-rna
- redir-attach-rej-gprs-ngs
- redir-attach-rej-comb-ngs
- redir-peroidic-rau-ngs
- redir-rau-gprs-intra-sgsn-rej-ngs
- redir-rau-comb-intra-sgsn-rej-ngs
- redir-rau-gprs-inter-sgsn-rej-ngs
- redir-rau-comb-inter-sgsn-rej-ngs
- redir-rau-gprs-inter-rat-ngs
- redir-rau-comb-inter-rat-ngs
- redir-rau-gprs-inter-serv-ngs
- redir-rau-comb-inter-serv-ngs
- redir-attach-rej-gprs-cpcr
- redir-attach-rej-comb-cpcr
- redir-peroidic-rau-cpcr
- redir-rau-gprs-intra-sgsn-rej-cpcr
- redir-rau-comb-intra-sgsn-rej-cpcr
- redir-rau-gprs-inter-sgsn-rej-cpcr

- redir-rau-comb-inter-sgsn-rej-cpcr
- redir-rau-gprs-inter-rat-cpcr
- redir-rau-comb-inter-rat-cpcr
- redir-rau-gprs-inter-serv-cpcr
- redir-rau-comb-inter-serv-cpcr
- redir-attach-rej-gprs-ur
- redir-attach-rej-comb-ur
- redir-peroidic-rau-ur
- redir-rau-gprs-intra-sgsn-rej-ur
- redir-rau-comb-intra-sgsn-rej-ur
- redir-rau-gprs-inter-sgsn-rej-ur
- redir-rau-comb-inter-sgsn-rej-ur
- redir-rau-gprs-inter-rat-ur
- redir-rau-comb-inter-rat-ur
- redir-rau-gprs-inter-serv-ur
- redir-rau-comb-inter-serv-ur
- 3G-attach-fail-iu_release-external
- 3G-attach-fail-iu_release-internal
- 3G-attach-fail-iu_release-comb-external
- 3G-attach-fail-iu_release-comb-internal
- 3G-actv-rej-network-failure-ext
- 3G-actv-rej-network-failure-int
- 3G-actv-rej-svc-opt-tmp-out-of-order-ext
- 3G-actv-rej-svc-opt-tmp-out-of-order-int
- 3G-actv-rej-unspecified-error-ext
- 3G-actv-rej-unspecified-error-int
- 3G-sec-actv-rej-unspecified-error-ext
- 3G-sec-actv-rej-unspecified-error-int
- 3G-actv-rej-insufficient-resources-ext
- 3G-actv-rej-insufficient-resources-int
- 3G-sec-actv-rej-insufficient-resources-ext
- 3G-sec-actv-rej-insufficient-resources-int
- 3G-total-actv-reject-internal
- 3G-total-actv-reject-external
- 2G-attach-rej-network-failure-ext
- 2G-attach-rej-network-failure-int
- 2G-comb-attach-rej-network-failure-ext
- 2G-comb-attach-rej-network-failure-int

- 3G-attach-rej-network-failure-ext
- 3G-attach-rej-network-failure-int
- 3G-comb-attach-rej-network-failure-ext
- 3G-comb-attach-rej-network-failure-int
- 2G-attach-fail-suspend-received
- 2G-attach-fail-bvc-rst-received
- 2G-attach-fail-sai-failure
- 2G-attach-fail-auth-tmr-expiry
- 2G-attach-fail-sgsn-init-detach
- 2G-attach-fail-plmn-check-failed
- 2G-attach-fail-identity-failure
- 2G-attach-fail-radio-status-cell-resel
- 2G-attach-fail-check-imei-failure
- 2G-attach-fail-rej-due-to-congestion
- 2G-attach-fail-camel-failure
- 2G-attach-fail-radio-status-bad
- 2G-attach-fail-t3350-expiry
- 2G-attach-fail-auth-failure
- 2G-attach-fail-glu-failure
- 2G-attach-fail-ms-init-detach
- 2G-attach-fail-opr-policy-failure
- 2G-attach-fail-cl-init-detach
- 2G-attach-fail-abort-on-attach
- 2G-attach-fail-attach-on-attach
- 2G-attach-fail-ready-tmr
- 2G-attach-fail-camel-srv-not-assoc
- 2G-attach-fail-p-tmsi-sign-mismatch
- 2G-attach-fail-xid-resp-failure
- 2G-attach-fail-internal-failure
- 2G-attach-fail-comb-suspend-received
- 2G-attach-fail-comb-bvc-rst-received
- 2G-attach-fail-comb-sai-failure
- 2G-attach-fail-comb-auth-tmr-expiry
- 2G-attach-fail-comb-sgsn-init-detach
- 2G-attach-fail-comb-plmn-check-failed
- 2G-attach-fail-comb-identity-failure
- 2G-attach-fail-comb-radio-status-cell-resel
- 2G-attach-fail-comb-check-imei-failure

- 2G-attach-fail-comb-rej-due-to-congestion
- 2G-attach-fail-comb-camel-failure
- 2G-attach-fail-comb-radio-status-bad
- 2G-attach-fail-comb-t3350-expiry
- 2G-attach-fail-comb-auth-failure
- 2G-attach-fail-comb-glu-failure
- 2G-attach-fail-comb-ms-init-detach
- 2G-attach-fail-comb-opr-policy-failure
- 2G-attach-fail-comb-cl-init-detach
- 2G-attach-fail-comb-abort-on-attach
- 2G-attach-fail-comb-attach-on-attach
- 2G-attach-fail-comb-ready-tmr
- 2G-attach-fail-comb-camel-srv-not-assoc
- 2G-attach-fail-comb-p-tmsi-sign-mismatch
- 2G-attach-fail-comb-xid-resp-failure
- 2G-attach-fail-comb-internal-failure

System Schema

- asnpc-cursess
- asnpc-curactive
- asnpc-ttlsetup
- asnpc-retriesexhaust
- asnpc-tidfail
- asnpc-luattempted
- asnpc-ludenied
- asnpc-lucomp
- asnpc-pagattempted
- asnpc-pagsucceeded
- asnpc-annoucetriggered
- cc-upd-titsutime
- cf-cat-backup-pkts-hit
- cf-cat-backup-pkts-block
- cf-cat-cdn-pkts-hit
- cf-cat-cdn-pkts-block
- cf-cat-photo-pkts-hit
- cf-cat-photo-pkts-block
- cf-cat-plag-pkts-hit
- cf-casngw-simple-ip-reanchored
- disc-reason-454

- disc-reason-455
- disc-reason-456
- disc-reason-457
- disc-reason-458
- disc-reason-459
- disc-reason-460
- disc-reason-461
- disc-reason-462
- disc-reason-463
- disc-reason-464
- disc-reason-465
- disc-reason-466
- disc-reason-467
- disc-reason-468
- disc-reason-469
- disc-reason-470
- disc-reason-471
- disc-reason-472
- disc-reason-473
- disc-reason-474
- disc-reason-475
- disc-reason-476
- disc-reason-477
- disc-reason-478
- disc-reason-479
- disc-reason-480
- disc-reason-481
- disc-reason-482
- disc-reason-483
- disc-reason-484
- disc-reason-485
- disc-reason-486
- disc-reason-487
- disc-reason-488
- disc-reason-489
- disc-reason-490
- disc-reason-491
- disc-reason-492

- disc-reason-493
- disc-reason-494
- disc-reason-495
- disc-reason-496
- disc-reason-497
- disc-reason-498
- disc-reason-499
- 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-attemptat-plag-pkts-block
- ipsecctrl-lte-template-reqs
- ipsecctrl-lte-template-unreg-reqs
- ipsecctrl-lte-map-reqs
- ipsecctrl-lte-map-est
- ipsecctrl-lte-map-del-reqs
- ipsecctrl-lte-map-failed
- ipsecctrl-lte-map-state-notif
- ipsecctrl-lte-ipsecmgr-death-notif
- ipsecctrl-lte-qos-maps

Modified Bulk Statistics

The following bulk statistics were modified in Release 12.0.

SGW Schema

The data type for the following bulk statistics changed from Int32 to Int64:

- datastat-uplink-qci1totbyte
- datastat-uplink-qci1totpkt
- datastat-uplink-qci2totbyte
- datastat-uplink-qci2totpkt
- datastat-uplink-qci3totbyte
- datastat-uplink-qci3totpkt
- datastat-uplink-qci4totbyte
- datastat-uplink-qci4totpkt
- datastat-uplink-qci5totbyte
- datastat-uplink-qci5totpkt
- datastat-uplink-qci6totbyte
- datastat-uplink-qci6totpkt
- datastat-uplink-qci7totbyte
- datastat-uplink-qci7totpkt
- datastat-uplink-qci8totbyte
- datastat-uplink-qci8totpkt
- datastat-uplink-qci9totbyte
- datastat-uplink-qci9totpkt
- datastat-uplink-othertotbyte
- datastat-uplink-othertotpkt
- datastat-downlink-qci1totbyte
- datastat-downlink-qci1totpkt
- datastat-downlink-qci2totbyte
- datastat-downlink-qci2totpkt
- datastat-downlink-qci3totbyte
- datastat-downlink-qci3totpkt
- datastat-downlink-qci4totbyte
- datastat-downlink-qci4totpkt
- datastat-downlink-qci5totbyte
- datastat-downlink-qci5totpkt
- datastat-downlink-qci6totbyte
- datastat-downlink-qci6totpkt
- datastat-downlink-qci7totbyte
- datastat-downlink-qci7totpkt

- datastat-downlink-qci8totbyte
- datastat-downlink-qci8totpkt
- datastat-downlink-qci9totbyte
- datastat-downlink-qci9totpkt
- datastat-downlink-othertotbyte
- datastat-downlink-othertotpkt

Obsoleted Bulk Statistics

The following bulk statistics were obsoleted in Release 12.0.

ECS Schema

- p2p-skype-voice-uplnk-bytes
- p2p-skype-voice-dwlnk-bytes
- p2p-skype-voice-uplnk-pkts
- p2p-skype-voice-dwlnk-pkts
- p2p-skype-non-voice-uplnk-bytes
- p2p-skype-non-voice-dwlnk-bytes
- p2p-skype-non-voice-uplnk-pkts
- p2p-skype-non-voice-dwlnk-pkts
- p2p-msn-voice-uplnk-bytes
- p2p-msn-voice-dwlnk-bytes
- p2p-msn-voice-uplnk-pkts
- p2p-msn-voice-dwlnk-pkts
- p2p-msn-non-voice-uplnk-bytes
- p2p-msn-non-voice-dwlnk-bytes
- p2p-msn-non-voice-uplnk-pkts
- p2p-msn-non-voice-dwlnk-pkts
- p2p-yahoo-voice-uplnk-bytes
- p2p-yahoo-voice-dwlnk-bytes
- p2p-yahoo-voice-uplnk-pkts
- p2p-yahoo-voice-dwlnk-pkts
- p2p-yahoo-non-voice-uplnk-bytes
- p2p-yahoo-non-voice-dwlnk-bytes
- p2p-yahoo-non-voice-uplnk-pkts
- p2p-yahoo-non-voice-dwlnk-pkts
- p2p-oscar-voice-uplnk-bytes
- p2p-oscar-voice-dwlnk-bytes
- p2p-oscar-voice-uplnk-pkts
- p2p-oscar-voice-dwlnk-pkts

- p2p-oscar-non-voice-uplnk-bytes
- p2p-oscar-non-voice-dwlnk-bytes
- p2p-oscar-non-voice-uplnk-pkts
- p2p-oscar-non-voice-dwlnk-pkts
- p2p-gtalk-voice-uplnk-bytes
- p2p-gtalk-voice-dwlnk-bytes
- p2p-gtalk-voice-uplnk-pkts
- p2p-gtalk-voice-dwlnk-pkts
- p2p-gtalk-non-voice-uplnk-bytes
- p2p-gtalk-non-voice-dwlnk-bytes
- p2p-gtalk-non-voice-uplnk-pkts
- p2p-gtalk-non-voice-dwlnk-pkts

MME Schema

- out-rau-ho-4gto3g-s3-attempted
- out-rau-ho-4gto3g-s3-success
- out-rau-ho-4gto3g-s3-failures
- in-tau-ho-2gto4g-gngp-attempted
- in-tau-ho-2gto4g-gngp-success
- in-tau-ho-2gto4g-gngp-failures
- out-rau-ho-4gto2g-gngp-attempted
- out-rau-ho-4gto2g-gngp-success
- out-rau-ho-4gto2g-gngp-failures

System Schema

- cf-dyn-rateblock
- cf-cat-adv-pkts-hit
- cf-cat-adv-pkts-block
- cf-cat-auct-pkts-hit
- cf-cat-auct-pkts-block
- cf-cat-clean-pkts-hit
- cf-cat-clean-pkts-block
- cf-cat-cporn-pkts-hit
- cf-cat-cporn-pkts-block
- cf-cat-esrb-pkts-hit
- cf-cat-esrb-pkts-block
- cf-cat-p2p-pkts-hit
- cf-cat-p2p-pkts-block
- cf-cat-radio-pkts-hit
- cf-cat-radio-pkts-block

- cf-cat-sftwre-pkts-hit
- cf-cat-sftwre-pkts-block
- cf-cat-spywre-pkts-hit
- cf-cat-spywre-pkts-block
- cf-cat-susp-pkts-hit
- cf-cat-susp-pkts-block

Bulk Statistic Enhancements in Release 12.1

This section lists bulk statistic additions and changes in Release 12.1.

- *New Bulk Statistics*
- *Modified Bulk Statistics*
- *Obsoleted Bulk Statistics*

New Bulk Statistics

Following new commands added for IPCF support in release 12.1:

Bulkstats Configuration Mode

- pcc-af schema
- pcc-policy schema
- pcc-sp-endpt schema
- pcc-service schema

pcc-af Schema

This is a new schema provided for PCC solution on IPCF node in Release 12.1.

- vpnname
- vpnid
- servname
- servid
- total-rx-inbound-msgs
- total-rx-outbound-msgs
- total-rx-aar-rcvd
- total-rx-aar-accept-sent
- total-rx-str-rcvd
- total-rx-srt-accept-sent
- total-rx-rar-sent
- total-rx-raa-rcvd
- total-rx-asr-sent
- total-rx-asa-rcvd

pcc-policy Schema

This is a new schema provided for PCC solution on IPCF node in Release 12.1.

- vpnname
- vpnid
- servname
- servid
- total-gx-inbound-msgs
- total-gx-outbound-msgs
- total-gx-ccr-rcvd
- total-gx-ccr-rej-sent
- total-gx-cca-accept-sent
- total-gx-ccri-rcvd
- total-gx-ccai-rej-sent
- total-gx-ccai-accept-sent
- total-gx-ccru-rcvd
- total-gx-ccru-rej-sent
- total-gx-ccru-accept-sent
- total-gx-ccrt-rcvd
- total-gx-ccrt-rej-sent
- total-gx-ccrt-accept-sent
- total-gx-unknown-ccr-rcvd
- total-gx-unknown-ccr-rej
- total-gx-rar-sent
- total-gx-raa-rcvd
- total-gx-rar-timeouts
- total-gx-raa-parse-success
- total-gx-raa-parse-fail
- 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

pcc-service Schema

This is a new schema provided for PCC solution on IPCF node in Release 12.1.

- vpnname
- vpnid

- servname
- servid
- total-gx-processed
- total-gy-processed
- total-spr-processed
- total-unknown-req
- total-pur-updates
- total-snr-requests
- total-pnr-requests
- total-profile-match-hits
- total-profile-match-miss
- total-quota-reports
- total-unknown-rt-req

pcc-sp-endpt Schema

This is a new schema provided for PCC solution on IPCF node in Release 12.1.

- vpnname
- vpnid
- endpt-name
- req-open
- req-close
- req-update-profile
- req-update-profile-answer
- req-user-data-req
- req-user-data-answer
- req-checkpoints
- req-recoveries
- req-user-data-query
- req-push-notif-req
- req-push-notif-answer
- req-subscr-notif-req
- req-subscr-notif-answer
- success-open
- success-close
- success-update-profile
- success-update-profile-answer
- success-user-data-req
- success-user-data-answer
- success-checkpoints

- success-recoveries
- success-user-data-query
- success-push-notif-req
- success-push-notif-answer
- success-subscr-notif-req
- success-subscr-notif-answer
- error-open
- error-close
- error-update-profile
- error-update-profile-answer
- error-user-data-req
- error-user-data-answer
- error-checkpoints
- error-recoveries
- error-user-data-query
- error-push-notif-req
- error-push-notif-answer
- error-subscr-notif-req
- error-subscr-notif-answer

Modified Bulk Statistics

The following bulk statistics were modified in Release 12.1.

None for this release.

Obsoleted Bulk Statistics

The following bulk statistics were obsoleted in Release 12.1.

None for this release.

Bulk Statistic Enhancements in Release 12.2

This section lists bulk statistic additions and changes in Release 12.2.

New Bulk Statistics

Support for the following bulk statistics were added in Release 12.2.

Context Schema

- nat-total-flows

- nat44-total-flows
- nat64-total-flows
- bypass-nat-total-flows
- bypass-nat-ipv4-total-flows
- bypass-nat-ipv6-total-flows

CSCF Schema

- srtp-sent
- srtp-recv
- srtcp-sent
- srtcp-recv

ECS Schema

- ecs-dns-learnt-ipv4-entries
- ecs-dns-flushed-ipv4-entries
- ecs-dns-replaced-ipv4-entries
- ecs-dns-overflown-ipv4-entries
- ecs-dns-learnt-ipv6-entries
- ecs-dns-flushed-ipv6-entries
- ecs-dns-replaced-ipv6-entries
- ecs-dns-overflown-ipv6-entries
- ip-charge-uplk-bytes
- ip-charge-dwnlk-bytes
- ip-charge-uplk-pkts
- ip-charge-dwnlk-pkts
- video-opt-total-transrated
- video-opt-transrated-sh263
- video-opt-transrated-h264
- video-opt-failed-sh263
- video-opt-failed-h264
- video-opt-total-input-bytes
- video-opt-total-input-bytes-sh263
- video-opt-total-input-bytes-h264
- video-opt-total-output-bytes
- video-opt-total-output-bytes-sh263
- video-opt-total-output-bytes-h264
- 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
- tcpprxy-usrtotsocksopn
- tcpprxy-inettotsocksopn
- tcpprxy-usrsockopnfail
- tcpprxy-inetsockopnfail
- tcpprxy-usrtotconnattmpt
- tcpprxy-inettotconnattmpt
- tcpprxy-usraccsucc
- tcpprxy-inetaccsucc
- tcpprxy-usraccfail
- tcpprxy-inetaccfail
- tcpprxy-usrcuropnsocks
- tcpprxy-inetcuropnsocks
- tcpprxy-usrcuralloctcpvect
- tcpprxy-inetcuralloctcpvect
- tcpprxy-usriptotpktsrcvd
- tcpprxy-inetiptotpktsrcvd
- tcpprxy-usriphdrerr
- tcpprxy-inetiphdrerr
- tcpprxy-usripunknownproto
- tcpprxy-inetipunknownproto
- tcpprxy-usripincomdiscpkts
- tcpprxy-inetipincomdiscpkts
- tcpprxy-usrtcpincomseg
- tcpprxy-inettcpincomseg
- tcpprxy-usrtcpincomerrseg
- tcpprxy-inettcpincomerrseg
- tcpprxy-usrtcpincomretransseg
- tcpprxy-inettcpincomretransseg
- tcpprxy-usrtcpoutgodataseg
- tcpprxy-inettcpoutgodataseg
- tcpprxy-usrtcpoutgorstseg
- tcpprxy-inettcpoutgorstseg
- tcpprxy-usrtcpoutgoretransseg

- tcpprxy-inettcpoutgoretransseg
- tcpprxy-usrtcpconnfail
- tcpprxy-inettcpconnfail
- tcpprxy-usrtcprstineststate
- tcpprxy-inettcprstineststate
- tcpprxy-usrtcpcurestconn
- tcpprxy-inettcpcurestconn
- tcpprxy-totprxyflows
- tcpprxy-currprxyflows
- tcpprxy-curactopnonusr
- tcpprxy-curactopnoninet
- tcpprxy-curpassopnonusr
- tcpprxy-curpassopnoninet
- tcpprxy-curestonboth
- tcpprxy-totpassopnsuccusr
- tcpprxy-totactopnsuccusr
- tcpprxy-totpassopnsuccinet
- tcpprxy-totactopnsuccinet
- tcpprxy-flowlimit
- tcpprxy-backloglimit
- tcpprxy-usrsocklimit
- tcpprxy-inetsocklimit
- tcpprxy-memthresholdlimit
- tcpprxy-incompactopn
- tcpprxy-incompassopn
- tcpprxy-usrsocknoerr
- tcpprxy-usrsocknopermissn
- tcpprxy-usrsocknomem
- tcpprxy-usrsocktoomanysocks
- tcpprxy-usrsockothers
- tcpprxy-inetsocknoerr
- tcpprxy-inetsocknopermissn
- tcpprxy-inetsocknomem
- tcpprxy-inetsocktoomanysock
- tcpprxy-inetsockothers
- tcpprxy-usrsockerropwouldblk
- tcpprxy-inetsockerropwouldblk
- tcpprxy-usrsockerropinprog

- tcpprxy-inetsockerropinprog
- tcpprxy-usrsockerrconnrstbypeer
- tcpprxy-inetsockerrconnrstbypeer
- tcpprxy-usrsockerrsendaftershtdwn
- tcpprxy-inetsockerrsendaftershtdwn
- tcpprxy-usrsockerroptmout
- tcpprxy-inetsockerroptmout
- tcpprxy-usrsockerrconnabort
- tcpprxy-inetsockerrconnabort
- tcpprxy-usrsockerrconnref
- tcpprxy-inetsockerrconnref
- tcpprxy-usrsockerrtoomanysocks
- tcpprxy-inetsockerrtoomanysocks
- tcpprxy-usrsockerrothers
- tcpprxy-inetsockerrothers
- tcpprxy-sockmigflowsinit
- tcpprxy-sockmigflowsmigattmpts
- tcpprxy-sockmigflowssucc
- tcpprxy-sockmigmemallocfail
- tcpprxy-sockmigpermissndenied
- tcpprxy-sockmigpossibtcpstatechng
- tcpprxy-sockmigpkttrimfail
- tcpprxy-sockmigothers
- tcpprxy-facacsmemlimit
- tcpprxy-facprxymemlimit
- tcpprxy-facflowspersublimit
- tcpprxy-factotprxyflowlimit
- video-readdress-get-req-redirected
- video-readdress-post-req-redirected
- video-readdress-other-req-redirected
- video-readdress-res-redirected
- video-readdress-req-with-xheader-inserted
- video-readdress-connect-failed-to-video-server
- video-readdress-upl-bytes-redirected
- video-readdress-upl-pkts-redirected
- video-readdress-dnl-bytes-redirected
- video-readdress-dnl-pkts-redirected
- p2p-meebo-voice-duration

- p2p-meebo-video-uplnk-bytes
- p2p-meebo-video-dwlnk-bytes
- p2p-meebo-video-uplnk-pkts
- p2p-meebo-video-dwlnk-pkts
- p2p-meebo-audio-uplnk-bytes
- p2p-meebo-audio-dwlnk-bytes
- p2p-meebo-audio-uplnk-pkts
- p2p-meebo-audio-dwlnk-pkts
- p2p-meebo-unclassified-uplnk-bytes
- p2p-meebo-unclassified-dwlnk-bytes
- p2p-meebo-unclassified-uplnk-pkts
- p2p-meebo-unclassified-dwlnk-pkts
- p2p-antsp2p-uplnk-bytes
- p2p-antsp2p-dwlnk-bytes
- p2p-antsp2p-uplnk-pkts
- p2p-antsp2p-dwlnk-pkts
- p2p-imo-uplnk-bytes
- p2p-imo-dwlnk-bytes
- p2p-imo-uplnk-pkts
- p2p-imo-dwlnk-pkts
- p2p-netmotion-uplnk-bytes
- p2p-netmotion-dwlnk-bytes
- p2p-netmotion-uplnk-pkts
- p2p-netmotion-dwlnk-pkts
- p2p-ogg-uplnk-bytes
- p2p-ogg-dwlnk-bytes
- p2p-ogg-uplnk-pkts
- p2p-ogg-dwlnk-pkts
- p2p-openvpn-uplnk-bytes
- p2p-openvpn-dwlnk-bytes
- p2p-openvpn-uplnk-pkts
- p2p-openvpn-dwlnk-pkts
- p2p-quicktime-uplnk-bytes
- p2p-quicktime-dwlnk-bytes
- p2p-quicktime-uplnk-pkts
- p2p-quicktime-dwlnk-pkts
- p2p-spotify-uplnk-bytes
- p2p-spotify-dwlnk-bytes

- p2p-spotify-uplnk-pkts
- p2p-spotify-dwlnk-pkts
- p2p-tango-uplnk-bytes
- p2p-tango-dwlnk-bytes
- p2p-tango-uplnk-pkts
- p2p-tango-dwlnk-pkts
- p2p-ultrabac-uplnk-bytes
- p2p-ultrabac-dwlnk-bytes
- p2p-ultrabac-uplnk-pkts
- p2p-ultrabac-dwlnk-pkts
- p2p-usenet-uplnk-bytes
- p2p-usenet-dwlnk-bytes
- p2p-usenet-uplnk-pkts
- p2p-usenet-dwlnk-pkts
- p2p-tunnelvoice-uplnk-bytes
- p2p-tunnelvoice-dwlnk-bytes
- p2p-tunnelvoice-uplnk-pkts
- p2p-tunnelvoice-dwlnk-pkts
- p2p-scydo-uplnk-bytes
- p2p-scydo-dwlnk-bytes
- p2p-scydo-uplnk-pkts
- p2p-scydo-dwlnk-pkts
- p2p-whatsapp-uplnk-bytes
- p2p-whatsapp-dwlnk-bytes
- p2p-whatsapp-uplnk-pkts
- p2p-whatsapp-dwlnk-pkts
- p2p-mypeople-uplnk-bytes
- p2p-mypeople-dwlnk-bytes
- p2p-mypeople-uplnk-pkts
- p2p-mypeople-dwlnk-pkts
- p2p-rdt-uplnk-bytes
- p2p-rdt-dwlnk-bytes
- p2p-rdt-uplnk-pkts
- p2p-rdt-dwlnk-pkts

eGTP-C Schema

- tun-sent-changenotfreq
- tun-sent-retranschangenotfreq
- tun-recv-changenotfreq

- tun-recv-retranschangenotfreq
- tun-sent-changenotfresp
- tun-sent-changenotfrespaccept
- tun-sent-changenotfrespdenied
- tun-sent-retranschangenotfresp
- tun-recv-changenotfresp
- tun-recv-changenotfrespaccept
- tun-recv-changenotfrespdenied
- tun-recv-creinddatafwdngrspaccept
- mobility-sent-ranInforelay
- mobility-recv-ranInforelay
- mobility-sent-configxfertun
- mobility-recv-configxfertun
- gtpv1path-recv-echoresp

HSGW Schema

- sessstat-totcur-pdn-ipv4
- sessstat-totcur-pdn-ipv6
- sessstat-totcur-pdn-ipv4v6
- ipv4-pdn-to-user-pkt
- ipv4-pdn-to-user-byte
- ipv4-pdn-from-user-pkt
- ipv4-pdn-from-user-byte
- ipv6-pdn-to-user-pkt
- ipv6-pdn-to-user-byte
- ipv6-pdn-from-user-pkt
- ipv6-pdn-from-user-byte
- ipv4v6-pdn-ipv4-to-user-pkt
- ipv4v6-pdn-ipv4-to-user-byte
- ipv4v6-pdn-ipv4-from-user-pkt
- ipv4v6-pdn-ipv4-from-user-byte
- ipv4v6-pdn-ipv6-to-user-pkt
- ipv4v6-pdn-ipv6-to-user-byte
- ipv4v6-pdn-ipv6-from-user-pkt
- ipv4v6-pdn-ipv6-from-user-byte

MME Schema

- dedi-brr-activation-nw-attempted
- dedi-brr-activation-nw-success
- dedi-brr-activation-nw-failures

- brr-deactivation-nw-attempted
- brr-deactivation-nw-success
- brr-deactivation-nw-failures
- emergency-pdn-connect-attempted
- emergency-pdn-connect-success
- emergency-pdn-connect-failures
- brr-modification-nw-attempted
- brr-modification-nw-success
- brr-modification-nw-failures
- sess-ecm-connect
- ecmevent-s1rel-loadbalance
- s1ap-transdata-cfgupd
- s1ap-transdata-cfgtfr
- s1ap-recdata-cfgupdfail
- s1ap-recdata-cfgupdack
- s1ap-recdata-enbcfgtfr
- s1ap-enodeb-assoc
- s1ap-err-unknownmme-ues1apid
- s1ap-err-unknownenb-ues1apid
- s1ap-err-unknownpair-ues1apid
- s1ap-err-tfr-synerr
- s1ap-err-semanticerr
- s1ap-err-msgnotcompatible
- s1ap-err-aserej
- s1ap-err-aseignore-notify
- s1ap-err-asefalsely-constrmsg
- paging-tai-list-success
- epsattach-emergency-attempted
- epsattach-emergency-success
- epsattach-emergency-failures
- emm-msgtx-imei-not-accept
- emm-msgtx-roaming-restrict-ta
- emm-msgtx-plmn-not-allow
- emm-msgtx-no-suitable-cell-ta
- emm-msgtx-ta-not-allow
- emm-msgtx-tau-imei-not-accept
- emm-msgtx-tau-roaming-restrict-ta
- emm-msgtx-tau-plmn-not-allow

- emm-msgtx-tau-no-suitable-cell-ta
- emm-msgtx-tau-ta-not-allow
- emm-msgtx-tau-cs-service-notif
- emm-msgrx-identity-resp
- emm-msgrx-ext-service-req
- esm-msgtx-brralloc-rej-insuff-resource
- esm-msgtx-brrmod-rej-insuff-resource
- esm-msgrx-deactivate-brr-accept
- out-rau-ho-4gto3g2g-gngp-attempted
- out-rau-ho-4gto3g2g-gngp-success
- out-rau-ho-4gto3g2g-gngp-failures
- in-tau-ho-2g3gto4g-gngp-attempted
- in-tau-ho-2g3gto4g-gngp-success
- in-tau-ho-2g3gto4g-gngp-failures
- out-rau-ho-4gto3g2g-s3-attempted
- out-rau-ho-4gto3g2g-s3-success
- out-rau-ho-4gto3g2g-s3-failures
- out-s1-ho-4gto3g-s3-attempted
- out-s1-ho-4gto3g-s3-success
- out-s1-ho-4gto3g-s3-failures
- in-tau-ho-2g3gto4g-s3-attempted
- in-tau-ho-2g3gto4g-s3-success
- in-tau-ho-2g3gto4g-s3-failures
- in-s1-ho-3gto4g-s3-attempted
- in-s1-ho-3gto4g-s3-success
- in-s1-ho-3gto4g-s3-failures
- out-s1-ho-4gto2g-s3-attempted
- out-s1-ho-4gto2g-s3-success
- out-s1-ho-4gto2g-s3-failures
- in-s1-ho-2gto4g-s3-attempted
- in-s1-ho-2gto4g-s3-success
- in-s1-ho-2gto4g-s3-failures
- s1-ho-4gto3g-cs-nodtm-sv-attempted
- s1-ho-4gto3g-cs-nodtm-sv-success
- s1-ho-4gto3g-cs-nodtm-sv-failures
- s1-ho-4gto3g-cs-sv-attempted
- s1-ho-4gto3g-cs-sv-success
- s1-ho-4gto3g-cs-sv-failures

- s1-ho-4gto3g-csps-sv-attempted
- s1-ho-4gto3g-csps-sv-success
- s1-ho-4gto3g-csps-sv-failures
- pdn-all
- pdn-connected
- pdn-idle
- pdn-emergency-all
- pdn-emergency-connected
- pdn-emergency-idle
- brr-all
- brr-connected
- brr-idle
- sess-call-all
- sess-call-connected
- sess-call-idle
- sess-emergency-call-all
- sess-emergency-call-connected
- sess-emergency-call-idle
- sess-unauth-call-all
- sess-unauth-call-connected
- sess-unauth-call-idle

NAT-Realm Schema

- nat-rlm-bytes-nat44-tx
- nat-rlm-bytes-nat64-tx
- nat-rlm-nat44-flows
- nat-rlm-nat64-flows
- nat-rlm-ip-denied-nat44
- nat-rlm-ip-denied-nat64
- nat-rlm-port-denied-nat44
- nat-rlm-port-denied-nat64

PGW Schema

- sessstat-bearact-emergency-def
- sessstat-bearact-emergency-auth-imsi-def
- sessstat-bearact-emergency-unauth-imsi-def
- sessstat-bearact-emergency-only-imei-def
- sessstat-bearact-emergency-ded
- sessstat-bearact-emergency-auth-imsi-ded
- sessstat-bearact-emergency-unauth-imsi-ded

- sessstat-bearact-emergency-only-imei-ded
- sessstat-bearsetup-emergency-def
- sessstat-bearsetup-emergency-auth-imsi-def
- sessstat-bearsetup-emergency-unauth-imsi-def
- sessstat-bearsetup-emergency-only-imei-def
- sessstat-bearsetup-emergency-ded
- sessstat-bearsetup-emergency-auth-imsi-ded
- sessstat-bearsetup-emergency-unauth-imsi-ded
- sessstat-bearsetup-emergency-only-imei-ded
- sessstat-bearrej-emergency-def
- sessstat-bearrej-emergency-ded
- ipv4-pdn-to-user-pkt
- ipv4-pdn-to-user-byte
- ipv4-pdn-from-user-pkt
- ipv4-pdn-from-user-byte
- ipv6-pdn-to-user-pkt
- ipv6-pdn-to-user-byte
- ipv6-pdn-from-user-pkt
- ipv6-pdn-from-user-byte
- ipv4v6-pdn-ipv4-to-user-pkt
- ipv4v6-pdn-ipv4-to-user-byte
- ipv4v6-pdn-ipv4-from-user-pkt
- ipv4v6-pdn-ipv4-from-user-byte
- ipv4v6-pdn-ipv6-to-user-pkt
- ipv4v6-pdn-ipv6-to-user-byte
- ipv4v6-pdn-ipv6-from-user-pkt
- ipv4v6-pdn-ipv6-from-user-byte

SGW Schema

- ipv4-pdn-to-user-pkt
- ipv4-pdn-to-user-byte
- ipv4-pdn-from-user-pkt
- ipv4-pdn-from-user-byte
- ipv6-pdn-to-user-pkt
- ipv6-pdn-to-user-byte
- ipv6-pdn-from-user-pkt
- ipv6-pdn-from-user-byte
- ipv4v6-pdn-ipv4-to-user-pkt
- ipv4v6-pdn-ipv4-to-user-byte

- ipv4v6-pdn-ipv4-from-user-pkt
- ipv4v6-pdn-ipv4-from-user-byte
- ipv4v6-pdn-ipv6-to-user-pkt
- ipv4v6-pdn-ipv6-to-user-byte
- ipv4v6-pdn-ipv6-from-user-pkt
- ipv4v6-pdn-ipv6-from-user-byte

System Schema

- cca-init-2001-rc
- cca-init-5003-rc
- cca-init-4011-rc
- cca-init-4012-rc
- cca-updt-2001-rc
- cca-updt-5003-rc
- cca-updt-4011-rc
- cca-updt-4012-rc
- disc-reason-490
- disc-reason-491
- disc-reason-492
- disc-reason-493
- disc-reason-494
- disc-reason-495
- disc-reason-496
- disc-reason-497
- disc-reason-498
- disc-reason-499
- disc-reason-500
- disc-reason-501
- disc-reason-502
- disc-reason-503
- disc-reason-504
- disc-reason-505
- disc-reason-506
- disc-reason-507
- disc-reason-508
- disc-reason-509
- disc-reason-510
- fail-action-term
- fail-action-contd

- ikev2-csa-delmultspisnt
- ikev2-csa-delmultspircv
- offline-active-sess
- sess-txpackets-umts
- sess-txbytes-umts
- sess-rxpackets-umts
- sess-rxbytes-umts
- sess-txpackets-gprs
- sess-txbytes-gprs
- sess-rxpackets-gprs
- sess-rxbytes-gprs
- sess-txpackets-lte
- sess-txbytes-lte
- sess-rxpackets-lte
- sess-rxbytes-lte
- sess-txpackets-ehrpd
- sess-txbytes-ehrpd
- sess-rxpackets-ehrpd
- sess-rxbytes-ehrpd
- sess-total-sessions-1xrtt
- sess-num-calls-arrived-1xrtt
- sess-num-calls-disconnected-1xrtt
- sess-total-sessions-evdorev0
- sess-num-calls-arrived-evdorev0
- sess-num-calls-disconnected-evdorev0
- sess-total-sessions-evdoreva
- sess-num-calls-arrived-evdoreva
- sess-num-calls-disconnected-evdoreva
- sess-total-sessions-evdora
- sess-num-calls-arrived-evdora
- sess-num-calls-disconnected-evdora
- sess-total-sessions-umts
- sess-num-calls-arrived-umts
- sess-ttlconnected-umts
- sess-num-calls-disconnected-umts
- sess-total-sessions-gprs
- sess-num-calls-arrived-gprs
- sess-ttlconnected-gprs

- sess-num-calls-disconnected-gprs
- sess-total-sessions-ehrpd
- sess-num-calls-arrived-ehrpd
- sess-ttlconnected-ehrpd
- sess-num-calls-disconnected-ehrpd
- sess-total-sessions-lte
- sess-num-calls-arrived-lte
- sess-ttlconnected-lte
- sess-num-calls-disconnected-lte

Modified Bulk Statistics

The following bulk statistics were modified in Release 12.2.

Card Schema

- All card statistics except CPU names now show "**Type:** Gauge".

GTPP Schema

- aaa-acct-arch (type = gauge)
- SGSN-change-limit

The above statistic was changed to the following:

- Serving-Node-change-limit

IMSA Schema

- dpca-cursess (type = gauge)

PGW Schema

- essstat-bearmodfail-uesyntft

The above statistic was changed to the following:

- sessstat-bearmodfail-uesyntft

Port Schema

- util-rx-curr (type = gauge)
- util-tx-curr (type = gauge)
- util-rx-5min (type = gauge)
- util-tx-5min (type = gauge)
- util-rx-15min (type = gauge)
- util-tx-15min (type = gauge)

SGW Schema

- sessstat-pdnsetuptype-ipv4
- sessstat-pdnsetuptype-ipv6

- sessstat-pdnsetuptype-ipv4v6

The statistics above were changed to the following (in order):

- sessstat-totcur-pdn-ipv4
- sessstat-totcur-pdn-ipv6
- sessstat-totcur-pdn-ipv4v6

The data type for the following bulk statistics changed from Int32 to Int64:

- datastat-uplink-qci1totpkt
- datastat-uplink-qci2totpkt
- datastat-uplink-qci3totpkt
- datastat-uplink-qci4totpkt
- datastat-uplink-qci5totpkt
- datastat-uplink-qci6totpkt
- datastat-uplink-qci7totpkt
- datastat-uplink-qci8totpkt
- datastat-uplink-qci9totpkt
- datastat-uplink-othertotbyte
- datastat-uplink-othertotpkt
- datastat-downlink-qci1totpkt
- datastat-downlink-qci2totpkt
- datastat-downlink-qci3totpkt
- datastat-downlink-qci4totpkt
- datastat-downlink-qci5totpkt
- datastat-downlink-qci6totpkt
- datastat-downlink-qci7totpkt
- datastat-downlink-qci8totpkt
- datastat-downlink-qci9totpkt
- datastat-downlink-othertotbyte
- datastat-downlink-othertotpkt

System Schema

- sess-ttlconnected (type = gauge)
- sess-curttlcalls (type = gauge)
- sess-cursipconn (type = gauge)
- sess-curmipconn (type = gauge)
- sess-curpmipconn (type = gauge)
- sess-curhaipsecconn (type = gauge)
- sess-ipsg-cur-archive-call (type = gauge)
- ipsg-total-archive-serv (type = gauge)

- sess-curnonanchorconn (type = gauge)
- flow-curdynamic (type = gauge)
- ssl-cachetotalsess (type = gauge)
- ggsn-cursgsnact (type = gauge)
- cf-cursub (type = gauge)
- disc-reason-489
- disc-reason-490
- disc-reason-491
- disc-reason-499
- disc-reason-500

Obsoleted Bulk Statistics

The following bulk statistics were obsoleted in Release 12.2.

eGTP-C Schema

- sess-cur
- tun-recv-updupanereq
- tun-recv-retransupduplanereq
- tun-sent-updupanereq
- tun-sent-updupanerespaccept
- tun-sent-updupanerespdenied
- tun-sent-deactbear
- tun-recv-deactbear
- tun-sent-deactbearfail
- tun-recv-deactbearfail
- gtpv1tun-sent-gpdu
- gtpv1tun-recv-gpdu
- gtpv1tun-txoctet
- gtpv1tun-rxoctet
- gtpv1tun-sent-gtpuerror
- gtpv1tun-recv-gtpuerror
- gtpv1tun-sent-endmarker
- gtpv1path-sent-hdrnotif
- gtpv1path-recv-hdrnotif

MME Schema

- emmevent-assoc-attempt
- emmevent-assoc-success
- emmevent-assoc-failure
- emmevent-associmsi-attempt

- emmevent-associmsi-success
- emmevent-associmsi-failure
- emmevent-assoclocguti-attempt
- emmevent-assoclocguti-success
- emmevent-assoclocguti-failure
- emmevent-assocnonlocguti-attempt
- emmevent-assocnonlocguti-success
- emmevent-assocnonlocguti-failure
- emmevent-tau-attempt
- emmevent-tau-success
- emmevent-tau-failure
- emmevent-detach-attempt
- emmevent-detach-success
- emmevent-detach-failure
- ecmevent-lastenb-success
- ecmevent-lasttai-success
- ecmevent-tailist-success
- ecmevent-paging-attempt
- ecmevent-paging-success
- ecmevent-paging-failure
- esmevent-pdndiscon-attempt
- esmevent-pdndiscon-success
- esmevent-pdndiscon-failure
- esmevent-dedbearact-attempt
- esmevent-dedbearact-success
- esmevent-dedbearact-failure
- esmevent-beardeact-attempt
- esmevent-beardeact-success
- esmevent-beardeact-failure
- esmctrlmsg-recv-cleartext
- esmctrlmsg-recv-integrity
- esmctrlmsg-recv-cipher
- esmctrlmsg-recv-accept
- esmctrlmsg-recv-discard
- esmctrlmsg-recv-denied
- esmctrlmsg-recv-deocdefail
- emmevent-tauattach-success
- emmevent-tauattach-failure

- emmevent-outrauho4g3g-success
- emmevent-outrauho4g3g-failure
- emmevent-outs1ho4g3g-success
- emmevent-outs1ho4g3g-failure
- emmevent-intauho3g4g-success
- emmevent-intauho3g4g-failure
- emmevent-ins1ho3g4g-success
- emmevent-ins1ho3g4g-failure
- emm-msgtx-imsi-detach
- emm-msgtx-tau-esm-failure
- esm-msgtx-brralloc-rej-pgw-rej
- esm-msgrx-discarded
- esm-msgrx-decode-failures
- out-rau-ho-4gto3g-gngp-attempted
- out-rau-ho-4gto3g-gngp-success
- out-rau-ho-4gto3g-gngp-failures
- in-tau-ho-2gto4g-gngp-attempted
- in-tau-ho-2gto4g-gngp-success
- in-tau-ho-2gto4g-gngp-failures
- in-tau-ho-3gto4g-gngp-attempted
- in-tau-ho-3gto4g-gngp-success
- in-tau-ho-3gto4g-gngp-failures
- out-rau-ho-4gto2g-gngp-attempted
- out-rau-ho-4gto2g-gngp-success
- out-rau-ho-4gto2g-gngp-failures
- out-rau-ho-4gto3g-s3-attempted
- out-rau-ho-4gto3g-s3-success
- out-rau-ho-4gto3g-s3-failures
- tot-pdn-current
- tot-pdn-max
- connected-pdn-current
- connected-pdn-max
- idle-pdn-current
- idle-pdn-max
- tot-brr-current
- tot-brr-max
- connected-brr-current
- connected-brr-max

- idle-brr-current
- idle-brr-max

Web Element Manager Path

Click Accounting | Bulk Statistics Configuration.

CDR Enhancements

This section lists changes to GTPP dictionaries in Release 12.x.

- *CDR Changes in Release 12.0*
- *CDR Changes in Release 12.2*

For detailed information on CDRs, refer to the *AAA and GTPP Interface Administration and Reference*.

CDR Changes in Release 12.0

This section lists GTPP dictionary changes in Release 12.0.

custom33 Dictionary

Previously, the APN OI and NI were length encoded and now the APN OI and NI are dot encoded.

custom24 Dictionary

The custom24 GTPP dictionary for P-GW CDRs now supports the following values in Charging Characteristics Selection Mode:

- servingNodeSupplied (0)
- homeDefault (3)
- roamingDefault (4)
- visitingDefault (5)
- AAASupplied (6)
- GWOverride (7)

Refer to the *AAA and GTPP Interface Administration and Reference* for details.

custom40 Dictionary

New custom40 GTPP dictionary for P-GW CDRs has been implemented.

Refer to the *AAA and GTPP Interface Administration and Reference* for details.

custom42 Dictionary

The new custom42 GTPP dictionary for P-GW CDRs has changed the encoding for MCC and MNC. Now, the encoding of MCC and MNC will be MCC2 MCC1 MNC3 MCC3 MNC2 MNC1 in PLM ID and ULI_MNC_MCC.

custom42 supports ASCII format P-GW CDRs.

Refer to the *AAA and GTPP Interface Administration and Reference* for details.

Length of charging rulebase-name in LOSDVs of eG-CDRs/P-GW-CDRs - Behavior Change

This change applies to all eG-CDR/PGW-CDR dictionaries.

The maximum character length of Charging Rulebase Name field in LOSDVs of eG-CDRs and P-GW-CDRs is now configurable. This change is now available in 12.0 and later releases.

In earlier releases, in case of custom5 or custom40 dictionaries, the rulebase name used to get trimmed to 16 characters. In other dictionaries the complete rulebase name used to appear in the LOSDVs.

A new CLI command now enables to configure maximum length of the rulebase name between 1 through 63 characters. If configured as 0 (zero), the rulebase name is not trimmed. This new CLI command is available at the context and GTPP group levels.

For more information, refer to the "**`gtpp egcdr rulebase-max-length`**" command in the *Context Configuration Mode Commands* and *GTPP Server Group Configuration Mode Commands* chapters of the *Command Line Interface Reference*.

qoSInformationNeg Field in all LOSDV - Behavior Change

This behavior change applies to the following ASN-encoded eG-CDR dictionaries:

- custom5
- custom6
- custom7
- custom8
- custom9
- custom12
- custom14
- custom15
- custom17
- custom19
- custom20
- custom22
- custom30
- custom33
- custom36
- custom37

In earlier releases, the "qosInformationNeg" field was included only once per rating group. This resulted in skipping this field for the next LOSDV that has the same rating group but different service ID.

With this change, in cases where the same rating group but different service ID combination is used, it is included once per rating_group+service_id combination.

network-initiated-pdp-context Field

This change applies to the following dictionaries:

- custom6

- custom8
- custom13
- custom24

Existing ‘network-initiated-pdp-context’ field has been implemented and will not populate if the PDP context is activated by the network side or if the customer is enabling a RAU from LTE to 3G.

Value of IMEISV Field in G-CDRs/eG-CDRs - Behavior Change

This change applies to all GTPP dictionaries used for GGSN.

In earlier releases, the IMEISV field accepted only digits 0 through 9. In the current release, apart from the digits 0 through 9, this field also accepts the alphabetic characters Athrough F. RADIUS will encode only 15 digit IMEISV if IMEI is 15 digits.

Command Enhancements

This section identifies GTPP command changes available in release 12.0.

gtpp egcdr rulebase-max-length

This command is used to configure the maximum length of charging rulebase name in LOSDVs of eG-CDRs/P-GW-CDRs to between 1 through 63 characters. If configured to 0 (zero) the rulebase name is not trimmed. This CLI command is now available in 12.0 and later releases.

Context Configuration Mode and GTPP Group Configuration Mode

gtpp egcdr rulebase-max-length *rulebase_name_max_length*

no gtpp egcdr rulebase-max-length

show gtpp group

This command displays information pertaining to all or the specified GTPP group. The output of this command now includes the following new field:

- Rulebase-max-length: Indicates the maximum length of charging rulebase name in LOSDVs of eG-CDRs/P-GW-CDRs, if configured to a non-zero value.

Exec Mode

show gtpp group [name *gtpp_group_name* **| all] [| { grep** *grep_options* **| more }]**

CDR Changes in Release 12.2

This section lists GTPP dictionary changes in Release 12.2.

Value of IMEISV Field in G-CDRs/eG-CDRs - Behavior Change

This change applies to all GTPP dictionaries used for GGSN.

In earlier releases, the IMEISV field accepted only digits 0 through 9. In the current release, apart from the digits 0 through 9, this field also accepts the alphabetic characters Athrough F. RADIUS will encode only 15 digit IMEISV if IMEI is 15 digits.

Diameter Attributes

This section lists additions and changes to Diameter attributes in Release 12.x.

Refer to the *AAA and GTPP Interface Administration and Reference* for details.

Diameter Attributes in Release 12.0

This section lists additions and changes to Diameter attributes in Release 12.0.

New Attributes

The following Diameter attributes are new in Release 12.0.

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*.

- CHAP-Auth
- CHAP-Challenge
- CHAP-Ident
- CHAP-Response
- IMSI-Unauthenticated-Flag
- SN-Charging-Id
- User-Password
- Wildcarded-Public-Identity

Modified Attributes

The following Diameter attribute was modified in Release 12.0.

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*.

- Experimental-Result-Code

Removed Attributes

The following Diameter attributes were removed in Release 12.0.

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*.

- EPS-Information
- HSGW-Address
- PGW-Address
- PGW-MCC-MNC
- SGW-Address

Diameter Attributes in Release 12.1

This section lists additions and changes to Diameter attributes in Release 12.1.

- *New Attributes*
- *Modified Attributes*
- *Removed Attributes*

New Attributes

The following Diameter attributes are new in Release 12.1.

None for this release.

Modified Attributes

The following Diameter attributes were modified in Release 12.1.

None for this release.

Removed Attributes

The following Diameter attributes were removed in Release 12.1.

None for this release.

Diameter Attributes in Release 12.2

This section lists additions and changes to Diameter attributes in Release 12.2.

- *New Attributes*
- *Modified Attributes*

- *Removed Attributes*

New Attributes

The following Diameter attributes are new in Release 12.2.

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*.

- Active-APN
- Age-Of-Location-Information
- Cause
- Cell-Global-Identity
- Charging-Characteristics-Selection-Mode
- Current-Location-Retrieved
- Destination-PGW
- EPS-Location-Information
- EPS-User-State
- EUTRAN-Cell-Global-Identity
- Error-Diagnostic
- Flow-Direction
- Geodetic-Information
- Geographical-Information
- ICS-Indicator
- IMS-Voice-Over-PS-Sessions-Supported
- Last-UE-Activity-Time
- Location-Area-Identity
- MME-Location-Information
- MME-User-State
- QoS-Rule-Base-Name
- Routing-Area-Identity
- SGSN-Location-Information
- SGSN-User-State
- Service-Area-Identity
- Tracking-Area-Identity
- User-State

Modified Attributes

The following Diameter attributes were modified in Release 12.2.

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*.

- Access-Network-Charging-Physical-Access-Id — The Vendor ID has been changed from 10415 to 8164.
- Access-Network-Charging-Physical-Access-Id-Realm — The Vendor ID has been changed from 10415 to 8164.
- Access-Network-Charging-Physical-Access-Id-Value — The Vendor ID has been changed from 10415 to 8164.
- AN-GW-Address — The M-flag has been changed from 0 to 1.
- APN-Aggregate-Max-Bitrate-DL — The M-flag has been changed from 0 to 1.
- APN-Aggregate-Max-Bitrate-UL — The M-flag has been changed from 0 to 1.
- CoA-IP-Address — The M-flag has been changed from 0 to 1.
- CoA-Information — The M-flag has been changed from 0 to 1.
- Default-EPS-Bearer-QoS — The M-flag has been changed from 0 to 1.
- Event-Report-Indication — The M-flag has been changed from 0 to 1.
- Flow-Information — The M-flag has been changed from 0 to 1 and the sub AVP “FLOW_DIRECTION” has been added.
- Flow-Label — The M-flag has been changed from 0 to 1.
- Packet-Filter-Content — The M-flag has been changed from 0 to 1.
- Packet-Filter-Identifier — The M-flag has been changed from 0 to 1.
- Packet-Filter-Information — The M-flag has been changed from 0 to 1.
- Packet-Filter-Operation — The M-flag has been changed from 0 to 1.
- QoS-Rule-Definition — Sub AVP “FLOW_INFORMATION” has been added.
- QoS-Rule-Install — The following sub AVPs QOS_RULE_NAME, QOS_RULE_BASE_NAME, RESOURCE_ALLOCATION_NOTIFICATION, RULE_ACTIVATION_TIME, RULE_DEACTIVATION_TIME have been added.
- QoS-Rule-Remove — Sub AVP “QOS_RULE_BASE_NAME” has been added.
- QoS-Rule-Report — Sub AVP “QOS_RULE_BASE_NAME” has been added.
- RAT-Type — The M-flag has been changed from 0 to 1.
- Resource-Allocation-Notification — The M-flag has been changed from 0 to 1.
- Security-Parameter-Index — The M-flag has been changed from 0 to 1.
- Specific-APN-Info — Sub AVP “VISITED_NETWORK_IDENTIFIER” has been added.
- Subscription-Data - Sub AVP “ICS_INDICATOR” has been added.

- Tunnel-Header-Filter — The M-flag has been changed from 0 to 1.
- Tunnel-Header-Length — The M-flag has been changed from 0 to 1.
- Tunnel-Information — The M-flag has been changed from 0 to 1.

Removed Attributes

The following Diameter attributes were removed in Release 12.2.

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*.

- HSGW-Address
- PGW-Address
- SGW-Address

RADIUS Attributes

This section lists additions and changes to RADIUS attributes in Release 12.x.

Refer to the *AAA and GTPP Interface Administration and Reference* for details.

RADIUS Attributes in Release 12.0

This section lists additions and changes to RADIUS attributes in Release 12.0.

New Attributes

The following RADIUS attributes are new in Release 12.0.

- Callback-Id
- SN-Handoff-Indicator
- SN-MIP-Send-Host-Config

Modified Attributes

The following RADIUS attributes were modified in Release 12.0.

- 3GPP2-IP-Services-Authorized
- 3GPP2-FEID
- 3GPP-Allocate-IPType
- Acct-Input-Packets
- Acct-Output-Packets
- Acct-Termination-Cause
- SN-Disconnect-Reason
- SN-Service-Type
- SN1-Disconnect-Reason
- WiMAX-PPAQ

Removed Attributes

The following RADIUS attributes were removed in Release 12.0.

None for this release.

RADIUS Attributes in Release 12.1

This section lists additions and changes to RADIUS attributes in Release 12.1.

- *New Attributes*
- *Modified Attributes*
- *Removed Attributes*

New Attributes

The following RADIUS attributes are new in Release 12.1.

None for this release.

Modified Attributes

The following RADIUS attributes were modified in Release 12.1.

None for this release.

Removed Attributes

The following RADIUS attributes were removed in Release 12.1.

None for this release.

RADIUS Attributes in Release 12.2

This section lists additions and changes to RADIUS attributes in Release 12.2.

- *New Attributes*
- *Modified Attributes*
- *Removed Attributes*

New Attributes

The following RADIUS attributes are new in Release 12.2.

- SN-LI-Dest-Address
- SN-User-Privilege
- SN1-LI-Dest-Address
- SN1-NAT-Port
- SN1-Roaming-Status

Modified Attributes

The following RADIUS attributes were modified in Release 12.2.

- 3GPP2-MEID — The description for this attribute has been changed.
- NAS-Port-Type — The following two Enum values “Wireless_XGP=36” and “Wireless_DHCP=41” have been added.
- SN-Disconnect-Reason — The following Enum values have been added:
  - sgsn-ptmsi-crunch = 499
  - 3Gto4G-context-replacement = 500
  - 4Gto3G-context-replacement = 501
  - mme-isr-sgsn-init-detach = 502

    - sgsn-isr-addl-ptmsi-rai = 503
    - sgsn-sgw-dbr-cause-isr-deact = 504
    - sgsn-isr-mme-init-detach = 505
    - mme-sgw-dbr-cause-isr-deact = 506
    - ptmsi-signature-mismatch = 507
    - camel-invalid-configuration = 508
    - sgsn-actv-reject-on-dns-failure = 509
    - mme-no-eps-bearers-activated=510
  - SN-Service-Type
  - SN1-Disconnect-Reason — The following Enum values have been added:
    - sgsn-ptmsi-crunch = 499
    - 3Gto4G-context-replacement = 500
    - 4Gto3G-context-replacement = 501
    - mme-isr-sgsn-init-detach = 502
    - sgsn-isr-addl-ptmsi-rai = 503
    - sgsn-sgw-dbr-cause-isr-deact = 504
    - sgsn-isr-mme-init-detach = 505
    - mme-sgw-dbr-cause-isr-deact = 506
    - ptmsi-signature-mismatch = 507
    - camel-invalid-configuration = 508
    - sgsn-actv-reject-on-dns-failure = 509
    - mme-no-eps-bearers-activated=510
  - SN1-NAT-Info-Record — The following sub-attributes “Calling-Station-Id” and “3GPP-Charging-Id” have been added.
  - SN1-Service-Type

Removed Attributes

The following RADIUS attributes were removed in Release 12.2.

None for this release.

Web Element Manager Enhancements

This section describes the Accounting enhancements made in Web Element Manager releases 12.0 and 12.2

Web Element Manager Accounting Enhancements in Release 12.0

The following WEM Accounting enhancements were made for Release 12.0.

Enhancements to View/Graph Bulk Statistics Feature

Previously, the Bulk Statistics Graphing feature allowed the user to view only 20 data sample points per page. This required the user to click to a second page if the number of data points exceeded 20.

The Bulk Statistics Graphing feature has been enhanced to allow the user to zoom in or out to view as few or as many graph data samplings on a single page. By providing a zoom a mechanism for viewing a large number of data samples on a single screen, users can more effective analyze the trend shown in the graph.

The slider mechanism is just below the graph display. By moving the slider control to the left or right, the user can decrease or increase the number of data samples shown.

Above the graph display, there are discrete zoom controls that allow the user to click to see one of the following graph views:

- 1hr: Display all data samples for a one-hour period.
- 3hr: Display all data samples for a three-hour period.
- 6hr: Display all data samples for a six-hour period.
- Max: Display all available data samples

IMPORTANT

The existing X-scale, X-scroll and Y-scale functionality have been replaced by the zoom in/zoom out feature. In addition, the Page size label has been removed, as the new zoom feature eliminates the need to view a graph over multiple pages.

Web Element Manager Path

- Accounting | View/Graph Bulk Statistics

DLCI_UTIL Bulk Statistics Enhancements

The following bulk statistic was added to the DLCI schema in WEM Release 12.0.

Table 4-1 DLCI Bulk Statistic Enhancement in WEM Release 12.0

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
DLCI Utilization Statistics	Path	dlci_util_path
	E1T1	dlci_util_ds1e1
	Timeslot	dlci_util_timeslot
	DLCI	dlci_util_dlci_no
DLCI Utilization Statistics /Average DLCI Utilization (Kbps)	Current Rx	dlci_util_dlci_curr_rx
	Current Tx	dlci_util_dlci_curr_tx
	5min Rx	dlci_util_dlci_5min_rx
	5min Tx	dlci_util_dlci_5min_tx
	15min Rx	dlci_util_dlci_15min_rx
	15min Tx	dlci_util_dlci_15min_tx

Web Element Manager Path

- Accounting | View/Graph Bulk Statistics

HNBGW RANAP Bulk Statistic Enhancements

The following bulk statistics were added to the HNBGW RANAP schema in WEM Release 12.0

Table 4-2 HNBGW RANAP Bulk Statistic Schema Enhancements in WEM Release 12.0

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
HNBGW RANAP Statistics / RANAP / CS Domain / Relocation Request	Relocation Request Tx	cs-reloc-req-tx
	RAB Setup Tx	cs-reloc-req-tx-rab-setup-tx
	Relocation Request ACK Rx	cs-reloc-req-ack-rx
	RAB Setup Success Rx	cs-reloc-req-ack-rx-rab-setup-succ-rx
	RAB Setup Fail Rx	cs-reloc-req-ack-rx-rab-setup-fail-rx
	RAB Setup Dropped	cs-reloc-req-ack-rx-rab-setup-dropped
	Relocation Detect Rx	cs-reloc-detect-rx
	Relocation Complete Rx	cs-reloc-comp-rx
	Relocation Failure Rx	cs-reloc-fail-rx
	Relocation Required Rx	cs-reloc-reqd-rx
HNBGW RANAP Statistics / RANAP / CS Domain / Relocation Request / UMTS AMR Codec	RAB Setup Tx	cs-reloc-req-amr-codec-rab-setup-tx
	RAB Setup Success Rx	cs-reloc-req-amr-codec-rab-setup-succ-rx
	RAB Setup Fail Rx	cs-reloc-req-amr-codec-rab-setup-fail-rx
HNBGW RANAP Statistics / RANAP / CS Domain / Relocation Request / UMTS AMR2 Codec	RAB Setup Tx	cs-reloc-req-amr2-codec-rab-setup-tx
	RAB Setup Success Rx	cs-reloc-req-amr2-codec-rab-setup-succ-rx
	RAB Setup Fail Rx	cs-reloc-req-amr2-codec-rab-setup-fail-rx
HNBGW RANAP Statistics / RANAP / CS Domain / Relocation Request / Other Codec	RAB Setup Tx	cs-reloc-req-other-codec-rab-setup-tx
	RAB Setup Success Rx	cs-reloc-req-no-codec-rab-setup-succ-rx
	RAB Setup Fail Rx	cs-reloc-req-no-codec-rab-setup-fail-rx

Table 4-2 HNBGW RANAP Bulk Statistic Schema Enhancements in WEM Release 12.0

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
HNBGW RANAP Statistics / RANAP / CS Domain / Relocation Request / Unknown Codec	RAB Setup Tx	cs-reloc-req-unknown-codec-rab-setup-tx
	RAB Setup Success Rx	cs-reloc-req-unknown-codec-rab-setup-succ-rx
	RAB Setup Fail Rx	cs-reloc-req-unknown-codec-rab-setup-fail-rx

Web Element Manager Path

- Accounting | Bulk Statistics Configuration | Schema Tab
- Accounting | View/Graph Bulk Statistics | Select Counters and Filters Parameters Tab

CS NW RANAP Bulk Statistic Enhancements

The following bulk statistics have been added to the CS NW RANAP schema in WEM Release 12.0.

Table 4-3 CS NW RANAP Bulk Statistic Enhancements in WEM Release 12.0

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
CS NW RANAP Statistics / RANAP / Relocation Request	Relocation Request Rx	reloc-req-rx
	RAB Setup Rx	reloc-req-rx-rab-setup-r
	Relocation Request ACK Tx	reloc-req-ack-tx
	RAB Setup Success Tx	reloc-req-ack-tx-rab-setup-succ-tx
	Total RAB Setup Fail Tx	reloc-req-ack-tx-tot-rab-setup-fail-tx
	RAB Setup Fail (Local) Tx	reloc-req-ack-tx-rab-setup-fail-local-tx
CS NW RANAP Statistics / RANAP / Relocation Request / Local Failure Cause / Radio Network Layer Cause	Invalid Rab Id	reloc-req-ack-local-fail-invalid-rab-id
	Interaction With Other Proc	reloc-req-ack-local-fail-interact-othr-proc
CS NW RANAP Statistics / RANAP / Relocation Request / Local Failure Cause / Transport Layer Cause	Sig Transport Resource Fail	reloc-req-ack-local-fail-sig-trans-res-fail
	Iu Transport Conn failed to Establish	reloc-req-ack-local-fail-iu-conn-fail-to-estab
CS NW RANAP Statistics / RANAP / Relocation Request / Local Failure Cause / Protocol Layer Cause	Transfer syntax error	reloc-req-ack-local-fail-trans-syn-err
	Abstract syntax error(Ignore)	reloc-req-ack-local-fail-abs-syn-err-ign
	Semantic error	reloc-req-ack-local-fail-semantic-err
	Abstract syntax error(Reject)	reloc-req-ack-local-fail-abs-syn-err-rej
	Msg not compatible with receiver state	reloc-req-ack-local-fail-msg-not-comp
	Abstract syntax error (Falsely constructed msg)	reloc-req-ack-local-fail-falsely-construct-msg
CS NW RANAP Statistics / RANAP / Relocation Request / Local Failure Cause / Miscellaneous Cause	No Resource Available	reloc-req-ack-local-fail-no-res-avalable
	Unspecified	reloc-req-ack-local-fail-unspecified
CS NW RANAP Statistics / RANAP / Relocation Request / Local Failure Cause / UMTS AMR Codec	RAB Setup Rx	reloc-req-amr-codec-rab-setup-rx
	RAB Setup Success Tx	reloc-req-amr-codec-rab-setup-succ-tx
	Total RAB Setup Fail Tx	reloc-req-amr-codec-tot-rab-setup-fail-tx
	RAB Setup Fail (Local) Tx	reloc-req-amr-codec-rab-setup-fail-local-tx

Table 4-3 CS NW RANAP Bulk Statistic Enhancements in WEM Release 12.0

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
CS NW RANAP Statistics / RANAP / Relocation Request / Local Failure Cause / UMTS AMR2 Codec	RAB Setup Rx	reloc-req-amr2-codec-rab-setup-rx
	RAB Setup Success Tx	reloc-req-amr2-codec-rab-setup-succ-tx
	Total RAB Setup Fail Tx	reloc-req-amr2-codec-tot-rab-setup-fail-t
	RAB Setup Fail (Local) Tx	reloc-req-amr2-codec-rab-setup-fail-local-tx
CS NW RANAP Statistics / RANAP / Relocation Request / Local Failure Cause / Other Codec	RAB Setup Rx	reloc-req-other-codec-rab-setup-rx
	RAB Setup Success Tx	reloc-req-other-codec-rab-setup-succ-tx
	Total RAB Setup Fail Tx	reloc-req-other-codec-tot-rab-setup-fail-tx
	RAB Setup Fail(Local) Tx	reloc-req-other-codec-rab-setup-fail-local-tx
CS NW RANAP Statistics / RANAP / Relocation Request / Local Failure Cause / No Codec	RAB Setup Rx	reloc-req-no-codec-rab-setup-rx
	RAB Setup Success Tx	reloc-req-no-codec-rab-setup-succ-tx
	Total RAB Setup Fail Tx	reloc-req-no-codec-tot-rab-setup-fail-tx
	RAB Setup Fail(Local) Tx	reloc-req-no-codec-rab-setup-fail-local-tx
CS NW RANAP Statistics / RANAP / Relocation Request / Local Failure Cause / Unknown Codec	RAB Setup Rx	reloc-req-unkwn-codec-rab-setup-succ-tx
	Total RAB Setup Fail Tx	reloc-req-unkwn-codec-tot-rab-setup-fail-tx
	RAB Setup Fail (Local) Tx	reloc-req-unkwn-codec-rab-setup-fail-local-tx
CS NW RANAP Statistics / RANAP / Relocation Request / Relocation	Relocation Detect Tx	reloc-detect-tx
	Relocation Complete Tx	reloc-comp-tx
	Total Relocation Failure Tx	total-reloc-fail-tx
	Relocation Failure (Local) Tx	reloc-fail-local-tx
	Relocation Required Tx	reloc-reqd-tx
CS NW RANAP Statistics / RANAP / Relocation Request / Relocation / Local Failure Cause / Radio Network Layer Cause	Invalid Rab Id	reloc-fail-tx-local-fail-invalid-rab-id
	Interaction With Other Proc	reloc-fail-tx-local-fail-interact-othr-proc
CS NW RANAP Statistics / RANAP / Relocation Request / Relocation / Local Failure Cause / Transport Layer Cause	Sig Transport Resource Fail	reloc-fail-tx-local-fail-sig-trans-res-fail
	Iu Transport Conn failed to Establish	reloc-fail-tx-local-fail-iu-conn-fail-to-estab
CS NW RANAP Statistics / RANAP / Relocation Request / Relocation / Local Failure Cause / Protocol Layer Cause	Transfer syntax error	reloc-fail-tx-local-fail-trans-syn-err
	Abstract syntax error (Ignore)	reloc-fail-tx-local-fail-abs-syn-err-ign
	Semantic error	reloc-fail-tx-local-fail-semantic-err
	Abstract syntax error(Reject)	reloc-fail-tx-local-fail-abs-syn-err-rej
	Msg not compatible with receiver state	reloc-fail-tx-local-fail-msg-not-comp
	Abstract syntax error (Falsely constructed msg)	reloc-fail-tx-local-fail-falsely-construct-msg
CS NW RANAP Statistics / RANAP / Relocation Request / Relocation / Local Failure Cause / Miscellaneous Cause	No Resource Available	reloc-fail-tx-local-fail-no-res-avalable
	Unspecified	reloc-fail-tx-local-fail-unspecified

Web Element Manager Path

- Accounting | Bulk Statistics Configuration | Schema Tab

- Accounting | View/Graph Bulk Statistics | Select Counters and Filters Parameters Tab

ASNGW Bulk Statistic Enhancements

The following bulk statistics were added to the ASNGW schema in WEM Release 12.0.

Table 4-4 ASNGW Bulk Statistic Schema Enhancements in WEM Release 12.0

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
ASNGW Statistics / R6 Messages / R6 Path Modification Request Messages	Total Sent	r6pathmodreq-totsent
	Retransmissions Sent	r6pathmodreq-retranssent
	Total Send Failures	r6pathmodreq-totsendfail
	Total Received	r6pathmodreq-totrec
	Total Accepted	r6pathmodreq-totacc
	Total Relayed	r6pathmodreq-totrelay
	Total Denied	r6pathmodreq-totdenied
	Total Discarded	r6pathmodreq-totdiscard
	Badly Formed	r6pathmodreq-badform
	Decode Error	r6pathmodreq-decodeerr
	Unspecified Error	r6pathmodreq-unspecerr
	Missing Mandatory TLV	r6pathmodreq-missmandtlv
	TLV Value Invalid	r6pathmodreq-tlvvalinval
	Unknown TLV	r6pathmodreq-unknowntlv
	Duplicate TLV Found	r6pathmodreq-duptlvfound
	No Session Found	r6pathmodreq-nosessfound
	Admin Prohibited	r6pathmodreq-adminprohib
	No Resource Drops	r6pathmodreq-noresourcedrop
	Transaction Id. Error	r6pathmodreq-transiderr

Table 4-4 ASNGW Bulk Statistic Schema Enhancements in WEM Release 12.0

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
ASNGW Statistics / R6 Messages / R6 Path Modification Response Messages	Total Sent	r6pathmodrsp-totsent
	Retransmissions Sent	r6pathmodrsp-retranssent
	Total Send Failures	r6pathmodrsp-totsendfail
	Total Received	r6pathmodrsp-totrec
	Total Accepted	r6pathmodrsp-totacc
	Total Relayed	r6pathmodrsp-totrelay
	Total Denied	r6pathmodrsp-totdenied
	Total Discarded	r6pathmodrsp-totdiscard
	Badly Formed	r6pathmodrsp-badform
	Decode Error	r6pathmodrsp-decodeerr
	Unspecified Error	r6pathmodrsp-unspecerr
	Missing Mandatory TLV	r6pathmodrsp-missmandtlv
	TLV Value Invalid	r6pathmodrsp-tlvvalinval
	Unknown TLV	r6pathmodrsp-unknowntlv
	Duplicate TLV Found	r6pathmodrsp-duptlvfound
	No Session Found	r6pathmodrsp-nosessfound
	Admin Prohibited	r6pathmodrsp-adminprohib
	No Resource Drops	r6pathmodrsp-noresourcedrop
	Transaction Id. Error	r6pathmodrsp-transiderr
ASNGW Statistics / R6 Messages / R6 Path Modification Ack Messages	Total Sent	r6pathmodack-totsent
	Retransmissions Sent	r6pathmodack-retranssent
	Total Send Failures	r6pathmodack-totsendfail
	Total Received	r6pathmodack-totrec
	Total Accepted	r6pathmodack-totacc
	Total Relayed	r6pathmodack-totrelay
	Total Denied	r6pathmodack-totdenied
	Total Discarded	r6pathmodack-totdiscard
	Badly Formed	r6pathmodack-badform
	Decode Error	r6pathmodack-decodeerr
	Unspecified Error	r6pathmodack-unspecerr
	Missing Mandatory TLV	r6pathmodack-missmandtlv
	TLV Value Invalid	r6pathmodack-tlvvalinval
	Unknown TLV	r6pathmodack-unknowntlv
	Duplicate TLV Found	r6pathmodack-duptlvfound
	No Session Found	r6pathmodack-nosessfound
	Admin Prohibited	r6pathmodack-adminprohib
	No Resource Drops	r6pathmodack-noresourcedrop
	Transaction Id. Error	r6pathmodack-transiderr

Table 4-4 ASNGW Bulk Statistic Schema Enhancements in WEM Release 12.0

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
ASNGW Statistics / R6 Messages / R4 Path Modification Request Messages	Total Sent	r4pathmodreq-totsent
	Retransmissions Sent	r4pathmodreq-retranssent
	Total Send Failures	r4pathmodreq-totsendfail
	Total Received	r4pathmodreq-totrec
	Total Accepted	r4pathmodreq-totacc
	Total Relayed	r4pathmodreq-totrelay
	Total Denied	r4pathmodreq-totdenied
	Total Discarded	r4pathmodreq-totdiscard
	Badly Formed	r4pathmodreq-badform
	Decode Error	r4pathmodreq-decodeerr
	Unspecified Error	r4pathmodreq-unspecerr
	Missing Mandatory TLV	r4pathmodreq-missmandtlv
	TLV Value Invalid	r4pathmodreq-tlvvalinval
	Unknown TLV	r4pathmodreq-unknowntlv
	Duplicate TLV Found	r4pathmodreq-duptlvfound
	No Session Found	r4pathmodreq-nosessfound
	Admin Prohibited	r4pathmodreq-adminprohib
	No Resource Drops	r4pathmodreq-noresourcedrop
	Transaction Id. Error	r4pathmodreq-transiderr
ASNGW Statistics / R6 Messages / R4 Path Modification Response Messages	Total Sent	r4pathmodrsp-totsent
	Retransmissions Sent	r4pathmodrsp-retranssent
	Total Send Failures	r4pathmodrsp-totsendfail
	Total Received	r4pathmodrsp-totrec
	Total Accepted	r4pathmodrsp-totacc
	Total Relayed	r4pathmodrsp-totrelay
	Total Denied	r4pathmodrsp-totdenied
	Total Discarded	r4pathmodrsp-totdiscard
	Badly Formed	r4pathmodrsp-badform
	Decode Error	r4pathmodrsp-decodeerr
	Unspecified Error	r4pathmodrsp-unspecerr
	Missing Mandatory TLV	r4pathmodrsp-missmandtlv
	TLV Value Invalid	r4pathmodrsp-tlvvalinval
	Unknown TLV	r4pathmodrsp-unknowntlv
	Duplicate TLV Found	r4pathmodrsp-duptlvfound
	No Session Found	r4pathmodrsp-nosessfound
	Admin Prohibited	r4pathmodrsp-adminprohib
	No Resource Drops	r4pathmodrsp-noresourcedrop
	Transaction Id. Error	r4pathmodrsp-transiderr

Table 4-4 ASNGW Bulk Statistic Schema Enhancements in WEM Release 12.0

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
ASNGW Statistics / R6 Messages / R4 Path Modification Ack Messages	Total Sent	r4pathmodack-totsent
	Retransmissions Sent	r4pathmodack-retranssent
	Total Send Failures	r4pathmodack-totsendfail
	Total Received	r4pathmodack-totrec
	Total Accepted	r4pathmodack-totacc
	Total Relayed	r4pathmodack-totrelay
	Total Denied	r4pathmodack-totdenied
	Total Discarded	r4pathmodack-totdiscard
	Badly Formed	r4pathmodack-badform
	Decode Error	r4pathmodack-decodeerr
	Unspecified Error	r4pathmodack-unspecerr
	Missing Mandatory TLV	r4pathmodack-missmandtlv
	TLV Value Invalid	r4pathmodack-tlvvalinval
	Unknown TLV	r4pathmodack-unknowntlv
	Duplicate TLV Found	r4pathmodack-duptlvfound
	No Session Found	r4pathmodack-nosessfound
	Admin Prohibited	r4pathmodack-adminprohib
	No Resource Drops	r4pathmodack-noresourcedrop
	Transaction Id. Error	r4pathmodack-transiderr
ASNGW Statistics / R6 Messages / R6 Capability Req Messages	Total Sent	r6capabilityreq-totsent
	Retransmissions Sent	r6capabilityreq-retranssent
	Total Send Failures	r6capabilityreq-totsendfail
	Total Received	r6capabilityreq-totrec
	Total Accepted	r6capabilityreq-totacc
	Total Relayed	r6capabilityreq-totrelay
	Total Denied	r6capabilityreq-totdenied
	Total Discarded	r6capabilityreq-totdiscard
	Badly Formed	r6capabilityreq-badform
	Decode Error	r6capabilityreq-decodeerr
	Unspecified Error	r6capabilityreq-unspecerr
	Missing Mandatory TLV	r6capabilityreq-missmandtlv
	TLV Value Invalid	r6capabilityreq-tlvvalinval
	Unknown TLV	r6capabilityreq-unknowntlv
	Duplicate TLV Found	r6capabilityreq-duptlvfound
	Admin Prohibited	r6capabilityreq-admprohibit
	No Resource Drops	r6capabilityreq-noresourcedrop
	Transaction Id. Error	r6capabilityreq-transiderr

Table 4-4 ASNGW Bulk Statistic Schema Enhancements in WEM Release 12.0

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
ASNGW Statistics / R6 Messages / R6 Capability Rsp Messages	Total Sent	r6capabilityrsp-totsent
	Retransmissions Sent	r6capabilityrsp-retranssent
	Total Send Failures	r6capabilityrsp-totsendfail
	Total Received	r6capabilityrsp-totrec
	Total Accepted	r6capabilityrsp-totacc
	Total Relayed	r6capabilityrsp-totrelay
	Total Denied	r6capabilityrsp-totdenied
	Total Discarded	r6capabilityrsp-totdiscard
	Badly Formed	r6capabilityrsp-badform
	Decode Error	r6capabilityrsp-decodeerr
	Unspecified Error	r6capabilityrsp-unspecerr
	Missing Mandatory TLV	r6capabilityrsp-missmandtlv
	TLV Value Invalid	r6capabilityrsp-tlvvalinval
	Unknown TLV	r6capabilityrsp-unknowntlv
	Duplicate TLV Found	r6capabilityrsp-duptlvfound
	No Session Found	r6capabilityrsp-nosessfound
	Admin Prohibited	r6capabilityrsp-admprohibit
	No Resource Drops	r6capabilityrsp-noresourcedrop
	Transaction Id. Error	r6capabilityrsp-transiderr
ASNGW Statistics / R6 Messages / R6 Capability Ack Messages	Total Sent	r6capabilityack-totsent
	Retransmissions Sent	r6capabilityack-retranssent
	Total Send Failures	r6capabilityack-totsendfail
	Total Received	r6capabilityack-totrec
	Total Accepted	r6capabilityack-totacc
	Total Relayed	r6capabilityack-totrelay
	Total Denied	r6capabilityack-totdenied
	Total Discarded	r6capabilityack-totdiscard
	Badly Formed	r6capabilityack-badform
	Decode Error	r6capabilityack-decodeerr
	Unspecified Error	r6capabilityack-unspecerr
	Missing Mandatory TLV	r6capabilityack-missmandtlv
	TLV Value Invalid	r6capabilityack-tlvvalinval
	Unknown TLV	r6capabilityack-unknowntlv
	Duplicate TLV Found	r6capabilityack-duptlvfound
	No Session Found	r6capabilityack-nosessfound
	Admin Prohibited	r6capabilityack-admprohibit
	No Resource Drops	r6capabilityack-noresourcedrop
	Transaction Id. Error	r6capabilityack-transiderr

Table 4-4 ASNGW Bulk Statistic Schema Enhancements in WEM Release 12.0

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
ASNGW Statistics / R6 Messages / R4 Capability Req Messages	Total Sent	r4capabilityreq-totsent
	Retransmissions Sent	r4capabilityreq-retranssent
	Total Send Failures	r4capabilityreq-totsendfail
	Total Received	r4capabilityreq-totrec
	Total Accepted	r4capabilityreq-totacc
	Total Relayed	r4capabilityreq-totrelay
	Total Denied	r4capabilityreq-totdenied
	Total Discarded	r4capabilityreq-totdiscard
	Badly Formed	r4capabilityreq-badform
	Decode Error	r4capabilityreq-decodeerr
	Unspecified Error	r4capabilityreq-unspecerr
	Missing Mandatory TLV	r4capabilityreq-missmandtlv
	TLV Value Invalid	r4capabilityreq-tlvvalinval
	Unknown TLV	r4capabilityreq-unknowntlv
	Duplicate TLV Found	r4capabilityreq-duptlvfound
	No Session Found	r4capabilityreq-nosessfound
	Admin Prohibited	r4capabilityreq-admprohibit
	No Resource Drops	r4capabilityreq-noresourcedrop
	Transaction Id. Error	r4capabilityreq-transiderr
ASNGW Statistics / R6 Messages / R4 Capability Rsp Messages	Total Sent	r4capabilityrsp-totsent
	Retransmissions Sent	r4capabilityrsp-retranssent
	Total Send Failures	r4capabilityrsp-totsendfail
	Total Received	r4capabilityrsp-totrec
	Total Accepted	r4capabilityrsp-totacc
	Total Relayed	r4capabilityrsp-totrelay
	Total Denied	r4capabilityrsp-totdenied
	Total Discarded	r4capabilityrsp-totdiscard
	Badly Formed	r4capabilityrsp-badform
	Decode Error	r4capabilityrsp-decodeerr
	Unspecified Error	r4capabilityrsp-unspecerr
	Missing Mandatory TLV	r4capabilityrsp-missmandtlv
	TLV Value Invalid	r4capabilityrsp-tlvvalinval
	Unknown TLV	r4capabilityrsp-unknowntlv
	Duplicate TLV Found	r4capabilityrsp-duptlvfound
	No Session Found	r4capabilityrsp-nosessfound
	Admin Prohibited	r4capabilityrsp-admprohibit
	No Resource Drops	r4capabilityrsp-noresourcedrop
	Transaction Id. Error	r4capabilityrsp-transiderr

Table 4-4 ASNGW Bulk Statistic Schema Enhancements in WEM Release 12.0

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
ASNGW Statistics / R6 Messages / R4 Capability Ack Messages	Total Sent	r4capabilityack-totsent
	Retransmissions Sent	r4capabilityack-retranssent
	Total Send Failures	r4capabilityack-totsendfail
	Total Received	r4capabilityack-totrec
	Total Accepted	r4capabilityack-totacc
	Total Relayed	r4capabilityack-totrelay
	Total Denied	r4capabilityack-totdenied
	Total Discarded	r4capabilityack-totdiscard
	Badly Formed	r4capabilityack-badform
	Decode Error	r4capabilityack-decodeerr
	Unspecified Error	r4capabilityack-unspecerr
	Missing Mandatory TLV	r4capabilityack-missmandtlv
	TLV Value Invalid	r4capabilityack-tlvvalinval
	Unknown TLV	r4capabilityack-unknowntlv
	Duplicate TLV Found	r4capabilityack-duptlvfound
	No Session Found	r4capabilityack-nosessfound
	Admin Prohibited	r4capabilityack-admprohibit
	No Resource Drops	r4capabilityack-noresourcedrop

Web Element Manager Path

- Accounting | Bulk Statistics Configuration | Schema Tab
- Accounting | View/Graph Bulk Statistics | Select Counters and Filters Parameters Tab

MME Bulk Statistics Enhancements

The following bulk statistic was added to the MME schema in WEM Release 12.0.

Table 4-5 MME Bulk Statistic Enhancement in WEM Release 12.0

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
MME Statistics / EMM Events / Outbound Relocations (using S1 HO procedures)	Failures	emmevent-outs1ho4g3g-failure

Web Element Manager Path

- Accounting | Bulk Statistics Configuration | Schema Tab
- Accounting | View/Graph Bulk Statistics | Select Counters and Filters Parameters Tab

System Bulk Statistics Enhancements

The following bulk statistics were added to the System schema in WEM Release 12.0.

Table 4-6 System Bulk Statistic Enhancements in WEM Release 12.0

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
System Statistics / Session Managers / Setup Time Statistics	16..18 sec	sess-setuptime-over16sec
System Statistics / CC Bad Answer Statistics	Auth-Application-Id	cc-badans-auth-appid
	Session-Id	cc-badans-sessid
	CC-Request-Number	cc-badans-cc-req-num
	CC-Request-Type	cc-badans-cc-req-type
	Origin-Host	cc-badans-origin-host
	Origin-Realm	cc-badans-origin-realm
	Parse-Message-Errors	cc-badans-parsemsg-err
	Parse-Mscc-Errors	cc-badans-parsemscc-err
	Misc	cc-badans-misc-err
System Statistics / Session Disconnect Reasons	CT-PMIP-RRQ-NVSE-Value-Change	disc-reason-427
	tcp-read-failed	disc-reason-428
	tcp-write-failed	disc-reason-429
	ssl-handshake-failed	disc-reason-430
	ssl-renegotiate-failed	disc-reason-431
	ssl-bad-message	disc-reason-432
	ssl-alert-received	disc-reason-433
	ssl-disconnect	disc-reason-434
	ssl-migration	disc-reason-435
	sgsn-ard-failure	disc-reason-436
	sgsn-camel-release	disc-reason-437

Web Element Manager Path

- Accounting | Bulk Statistics Configuration | Schema Tab
- Accounting | View/Graph Bulk Statistics | Select Counters and Filters Parameters Tab

SGW Bulk Statistic Enhancements in Release 12.0.

The following table lists the SGW bulk statistics added in WEM Release 12.0.

Table 4-7 SGW Bulk Statistic Enhancements in WEM Release 12.0

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
SGW Statistics / Session Level Statistics / PDNs Released Reason	S4 Error Ind	sessstat-pdnrelrsn-s4err
	S12 Error Ind	sessstat-pdnrelrsn-s12err
	Path Failure S4	sessstat-pdnrelrsn-pathfail-S4
	Path Failure S12	sessstat-pdnrelrsn-pathfail-S12
	Path Failure S4-U	sessstat-pdnrelrsn-pathfail-S4-u
SGW Statistics / Bearer Level Statistics / Dedicated Bearers Released Reason	S4 Error Ind	totepsbearrel-dedrsn-s4err
	S12 Error Ind	totepsbearrel-dedrsn-s12err

Table 4-7 SGW Bulk Statistic Enhancements in WEM Release 12.0

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
SGW Statistics / Bearer Level Statistics / Dedicated Bearers Released Reason (con't)	Path Failure S12	totepsbearrel-dedrsn-pathfail-s12
	Path Failure S4-U	totepsbearrel-dedrsn-pathfail-s4-u
SGW Statistics / Inter-SGW Handover Statistics / X2 Based	Success	intersgwhaovstat-pdnin-x2-success
	Fail	intersgwhaovstat-pdnin-x2-fail
SGW Statistics / Inter-SGW Handover Statistics / Idle-mode TAU	Success	intersgwhaovstat-pdnin-idletau-success
	Fail	intersgwhaovstat-pdnin-idletau-fail
SGW Statistics / Inter-SGW Handover Statistics / S1 Based	Success	intersgwhaovstat-pdnin-s1-success
	Fail	intersgwhaovstat-pdnin-s1-fail
SGW Statistics / Inter-SGW Handover Statistics / Inter System	Fail	intersgwhaovstat-intersystem-fail
	Success	intersgwhaovstat-intersystem-success
	Fail	intersgwhaovstat-intersystem-fail
SGW Statistics / Intra-SGW Handover Statistics / Intra-MME	Success	intersgwhaovstat-intra-intramme-success
	Fail	intersgwhaovstat-intra-intramme-fail
SGW Statistics / Intra-SGW Handover Statistics / Inter-MME	Success	intersgwhaovstat-intra-intermme-success
	Fail	intersgwhaovstat-intra-intermme-fail

Table 4-7 SGW Bulk Statistic Enhancements in WEM Release 12.0

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
SGW Statistics / S1U Total Data Statistics / Uplink	Pkts	s1u-uplnk-packets
	Bytes	s1u-uplnk-bytes
	Dropped Pkts	s1u-uplnk-dropped-packets
	Dropped Bytes	s1u-uplnk-dropped-bytes
	Bytes QCI 1	s1u-uplnk-qci1totbyte
	Pkts QCI 1	s1u-uplnk-qci1totpkt
	Bytes QCI 2	s1u-uplnk-qci2totbyte
	Pkts QCI 2	s1u-uplnk-qci2totpkt
	Bytes QCI 3	s1u-uplnk-qci3totbyte
	Pkts QCI 3	s1u-uplnk-qci3totpkt
	Bytes QCI 4	s1u-uplnk-qci4totbyte
	Pkts QCI 4	s1u-uplnk-qci4totpkt
	Bytes QCI 5	s1u-uplnk-qci5totbyte
	Pkts QCI 5	s1u-uplnk-qci5totpkt
	Bytes QCI 6	s1u-uplnk-qci6totbyte
	Pkts QCI 6	s1u-uplnk-qci6totpkt
	Bytes QCI 7	s1u-uplnk-qci7totbyte
	Pkts QCI 7	s1u-uplnk-qci7totpkt
	Bytes QCI 8	s1u-uplnk-qci8totbyte
	Pkts QCI 8	s1u-uplnk-qci8totpkt
	Bytes QCI 9	s1u-uplnk-qci9totbyte
	Pkts QCI 9	s1u-uplnk-qci9totpkt
	Bytes Non-Std QCI	s1u-uplnk-othertotbyte
	Pkts Non-Std QCI	s1u-uplnk-othertotpkt
	Dropped Bytes QCI 1	s1u-uplnk-drop-qci1totbyte
	Dropped Pkts QCI 1	s1u-uplnk-drop-qci1totpkt
	Dropped Bytes QCI 1	s1u-uplnk-drop-qci1totbyte
	Dropped Bytes QCI 2	s1u-uplnk-drop-qci2totbyte
	Dropped Pkts QCI 2	s1u-uplnk-drop-qci2totpkt
	Dropped Bytes QCI 3	s1u-uplnk-drop-qci3totbyte
	Dropped Pkts QCI 3	s1u-uplnk-drop-qci3totpkt

Table 4-7 SGW Bulk Statistic Enhancements in WEM Release 12.0

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
SGW Statistics / S1U Total Data Statistics / Uplink (con't)	Dropped Bytes QCI 4	s1u-uplnk-drop-qci4totbyte
	Dropped Pkts QCI 4	s1u-uplnk-drop-qci4totpkt
	Dropped Bytes QCI 5	s1u-uplnk-drop-qci5totbyte
	Dropped Pkts QCI 5	s1u-uplnk-drop-qci5totpkt
	Dropped Pkts QCI 6	s1u-uplnk-drop-qci6totpkt
	Dropped Bytes QCI 6	s1u-uplnk-drop-qci6totbyte
	Dropped Pkts QCI 7	s1u-uplnk-drop-qci7totpkt
	Dropped Bytes QCI 7	s1u-uplnk-drop-qci7totbyte
	Dropped Pkts QCI 8	s1u-uplnk-drop-qci8totpkt
	Dropped Bytes QCI 8	s1u-uplnk-drop-qci8totbyte
	Dropped Pkts QCI 9	s1u-uplnk-drop-qci9totpkt
	Dropped Bytes QCI 9	s1u-uplnk-drop-qci9totbyte
	Dropped Pkts Non-Std QCI	s1u-uplnk-drop-otherpkt
	Dropped Bytes Non-Std QCI	s1u-uplnk-drop-othertotbyte
SGW Statistics / S1U Total Data Statistics / Downlink	Pkts	s1u-downlnk-packets
	Bytes	s1u-downlnk-bytes
	Dropped Pkts	s1u-downlnk-dropped-packets
	Dropped Bytes	s1u-downlnk-dropped-bytes
	Bytes QCI 1	s1u-downlnk-qci1totbyte
	Pkts QCI 1	s1u-downlnk-qci1totpkt
	Bytes QCI 2	s1u-downlnk-qci2totbyte
	Pkts QCI 2	s1u-downlnk-qci2totpkt
	Bytes QCI 3	s1u-downlnk-qci3totbyte
	Pkts QCI 3	s1u-downlnk-qci3totpkt
	Bytes QCI 4	s1u-downlnk-qci4totbyte
	Pkts QCI 4	s1u-downlnk-qci4totpkt
	Bytes QCI 5	s1u-downlnk-qci5totbyte
	Pkts QCI 5	s1u-downlnk-qci5totpkt
	Bytes QCI 6	s1u-downlnk-qci6totbyte
	Pkts QCI 6	s1u-downlnk-qci6totpkt
	Bytes QCI 7	s1u-downlnk-qci7totbyte
	Pkts QCI 7	s1u-downlnk-qci7totpkt
	Bytes QCI 8	s1u-downlnk-qci8totbyte
	Pkts QCI 8	s1u-downlnk-qci8totpkt
	Bytes QCI 9	s1u-downlnk-qci9totbyte
	Pkts QCI 9	s1u-downlnk-qci9totpkt
	Bytes Non-Std QCI	s1u-downlnk-othertotbyte
	Pkts Non-Std QCI	s1u-downlnk-othertotpkt
	Dropped Bytes QCI 1	s1u-downlnk-drop-qci1totbyte

Table 4-7 SGW Bulk Statistic Enhancements in WEM Release 12.0

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
SGW Statistics / S1U Total Data Statistics / Downlink (con't)	Dropped Pkts QCI 1	s1u-downlnk-drop-qci1totpkt
	Dropped Bytes QCI 2	s1u-downlnk-drop-qci2totbyte
	Dropped Pkts QCI 2	s1u-downlnk-drop-qci2totpkt
	Dropped Bytes QCI 3	s1u-downlnk-drop-qci3totbyte
	Dropped Pkts QCI 3	s1u-downlnk-drop-qci3totpkt
	Dropped Bytes QCI 4	s1u-downlnk-drop-qci4totbyte
	Dropped Pkts QCI 4	s1u-downlnk-drop-qci4totpkt
	Dropped Bytes QCI 5	s1u-downlnk-drop-qci5totbyte
	Dropped Pkts QCI 5	s1u-downlnk-drop-qci5totpkt
	Dropped Bytes QCI 6	s1u-downlnk-drop-qci6totbyte
	Dropped Pkts QCI 6	s1u-downlnk-drop-qci6totpkt
	Dropped Bytes QCI 7	s1u-downlnk-drop-qci7totbyte
	Dropped Pkts QCI 7	s1u-downlnk-drop-qci7totpkt
	Dropped Bytes QCI 8	s1u-downlnk-drop-qci8totbyte
	Dropped Pkts QCI 8	s1u-downlnk-drop-qci8totpkt
	Dropped Bytes QCI 9	s1u-downlnk-drop-qci9totbyte
	Dropped Pkts QCI 9	s1u-downlnk-drop-qci9totpkt
	Dropped Bytes Non-Std QCI	s1u-downlnk-drop-othertotbyte
	Dropped Pkts Non-Std QCI	s1u-downlnk-drop-othertotpkt
SGW Statistics / S4U Total Data Statistics / Uplink	Pkts	s4u-uplnk-packets
	Bytes	s4u-uplnk-bytes
	Dropped Pkts	s4u-uplnk-dropped-packets
	Dropped Bytes	s4u-uplnk-dropped-bytes
	Bytes QCI 1	s4u-uplnk-qci1totbyte
	Pkts QCI 1	s4u-uplnk-qci1totpkt
	Bytes QCI 2	s4u-uplnk-qci2totbyte
	Pkts QCI 2	s4u-uplnk-qci2totpkt
	Bytes QCI 3	s4u-uplnk-qci3totbyte
	Pkts QCI 3	s4u-uplnk-qci3totpkt
	Bytes QCI 4	s4u-uplnk-qci4totbyte
	Pkts QCI 4	s4u-uplnk-qci4totpkt
	Bytes QCI 5	s4u-uplnk-qci5totbyte
	Pkts QCI 5	s4u-uplnk-qci5totpkt
	Bytes QCI 6	s4u-uplnk-qci6totbyte
	Pkts QCI 6	s4u-uplnk-qci6totpkt
	Bytes QCI 7	s4u-uplnk-qci7totbyte
	Pkts QCI 7	s4u-uplnk-qci7totpkt
	Bytes QCI 8	s4u-uplnk-qci8totbyte

Table 4-7 SGW Bulk Statistic Enhancements in WEM Release 12.0

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
SGW Statistics / S4U Total Data Statistics / Uplink (con't)	Pkts QCI 8	s4u-uplnk-qci8totpkt
	Bytes QCI 9	s4u-uplnk-qci9totbyte
	Pkts QCI 9	s4u-uplnk-qci9totpkt
	Bytes Non-Std QCI	s4u-uplnk-othertotbyte
	Pkts Non-Std QCI	s4u-uplnk-othertotpkt
	Dropped Bytes QCI 1	s4u-uplnk-drop-qci1totbyte
	Dropped Pkts QCI 1	s4u-uplnk-drop-qci1totpkt
	Dropped Bytes QCI 2	s4u-uplnk-drop-qci2totbyte
	Dropped Pkts QCI 2	s4u-uplnk-drop-qci2totpkt
	Dropped Bytes QCI 3	s4u-uplnk-drop-qci3totbyte
	Dropped Pkts QCI 3	s4u-uplnk-drop-qci3totpkt
	Dropped Bytes QCI 4	s4u-uplnk-drop-qci4totbyte
	Dropped Pkts QCI 4	s4u-uplnk-drop-qci4totpkt
	Dropped Bytes QCI 5	s4u-uplnk-drop-qci5totbyte
	Dropped Pkts QCI 5	s4u-uplnk-drop-qci5totpkt
	Dropped Bytes QCI 6	s4u-uplnk-drop-qci6totbyte
	Dropped Pkts QCI 6	s4u-uplnk-drop-qci6totpkt
	Dropped Bytes QCI 7	s4u-uplnk-drop-qci7totbyte
	Dropped Pkts QCI 7	s4u-uplnk-drop-qci7totpkt
	Dropped Bytes QCI 8	s4u-uplnk-drop-qci8totbyte
	Dropped Pkts QCI 8	s4u-uplnk-drop-qci8totpkt
	Dropped Bytes QCI 9	s4u-uplnk-drop-qci9totbyte
	Dropped Pkts QCI 9	s4u-uplnk-drop-qci9totpkt
	Dropped Bytes Non-Std QCI	s4u-uplnk-drop-othertotbyte
	Dropped Pkts Non-Std QCI	s4u-uplnk-drop-otherpkt
SGW Statistics / S4U Total Data Statistics / Downlink	Pkts	s4u-downlnk-packets
	Bytes	s4u-downlnk-bytes
	Dropped Pkts	s4u-downlnk-dropped-packets
	Dropped Bytes	s4u-downlnk-dropped-bytes
	Bytes QCI 1	s4u-downlnk-qci1totbyte
	Pkts QCI 1	s4u-downlnk-qci1totpkt
	Bytes QCI 2	s4u-downlnk-qci2totbyte
	Pkts QCI 2	s4u-downlnk-qci2totpkt
	Bytes QCI 3	s4u-downlnk-qci3totbyte
	Pkts QCI 3	s4u-downlnk-qci3totpkt
	Bytes QCI 4	s4u-downlnk-qci4totbyte
	Pkts QCI 4	s4u-downlnk-qci4totpkt
	Bytes QCI 5	s4u-downlnk-qci5totbyte
	Pkts QCI 5	s4u-downlnk-qci5totpkt

Table 4-7 SGW Bulk Statistic Enhancements in WEM Release 12.0

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
SGW Statistics / S4U Total Data Statistics / Downlink (con't)	Bytes QCI 6	s4u-downlnk-qci6totbyte
	Pkts QCI 6	s4u-downlnk-qci6totpkt
	Bytes QCI 7	s4u-downlnk-qci7totbyte
	Pkts QCI 7	s4u-downlnk-qci7totpkt
	Bytes QCI 8	s4u-downlnk-qci8totbyte
	Pkts QCI 8	s4u-downlnk-qci8totpkt
	Bytes QCI 9	s4u-downlnk-qci9totbyte
	Pkts QCI 9	s4u-downlnk-qci9totpkt
	Bytes Non-Std QCI	s4u-downlnk-othertotbyte
	Pkts Non-Std QCI	s4u-downlnk-othertotpkt
	Dropped Bytes QCI 1	s4u-downlnk-drop-qci1totbyte
	Dropped Pkts QCI 1	s4u-downlnk-drop-qci1totpkt
	Dropped Bytes QCI 2	s4u-downlnk-drop-qci2totbyte
	Dropped Pkts QCI 2	s4u-downlnk-drop-qci2totpkt
	Dropped Bytes QCI 3	s4u-downlnk-drop-qci3totbyte
	Dropped Pkts QCI 3	s4u-downlnk-drop-qci3totpkt
	Dropped Bytes QCI 4	s4u-downlnk-drop-qci4totbyte
	Dropped Pkts QCI 4	s4u-downlnk-drop-qci4totpkt
	Dropped Bytes QCI 5	s4u-downlnk-drop-qci5totbyte
	Dropped Pkts QCI 5	s4u-downlnk-drop-qci5totpkt
	Dropped Bytes QCI 6	s4u-downlnk-drop-qci6totbyte
	Dropped Pkts QCI 6	s4u-downlnk-drop-qci6totpkt
	Dropped Bytes QCI 7	s4u-downlnk-drop-qci7totbyte
	Dropped Pkts QCI 7	s4u-downlnk-drop-qci7totpkt
	Dropped Bytes QCI 8	s4u-downlnk-drop-qci8totbyte
	Dropped Pkts QCI 8	s4u-downlnk-drop-qci8totpkt
	Dropped Bytes QCI 9	s4u-downlnk-drop-qci9totbyte
SGW Statistics / S4U Total Data Statistics / Downlink (con't)	Dropped Pkts QCI 9	s4u-downlnk-drop-qci9totpkt
	Dropped Bytes Non-Std QCI	s4u-downlnk-drop-othertotbyte
	Dropped Pkts Non-Std QCI	s4u-downlnk-drop-othertotpkt
SGW Statistics / S5 Total Data Statistics / Uplink	Pkts	s5-uplnk-packets
	Bytes	s5-uplnk-bytes
	Dropped Pkts	s5-uplnk-dropped-packets
	Dropped Bytes	s5-uplnk-dropped-bytes
	Pkts QCI 1	s5-uplnk-qci1totpkt
	Pkts QCI 2	s5-uplnk-qci2totpkt
	Pkts QCI 3	s5-uplnk-qci3totpkt
	Pkts QCI 4	s5-uplnk-qci4totpkt
	Pkts QCI 5	s5-uplnk-qci5totpkt

Table 4-7 SGW Bulk Statistic Enhancements in WEM Release 12.0

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
SGW Statistics / S5 Total Data Statistics / Uplink (con't)	Pkts QCI 6	s5-uplnk-qci6totpkt
	Pkts QCI 7	s5-uplnk-qci7totpkt
	Pkts QCI 8	s5-uplnk-qci8totpkt
	Pkts QCI 9	s5-uplnk-qci9totpkt
	Pkts Non-Std QCI	s5-uplnk-othertotpkt
	Bytes QCI 1	s5-uplnk-qci1totbyte
	Bytes QCI 2	s5-uplnk-qci1totbyte
	Bytes QCI 3	s5-uplnk-qci1totbyte
	Bytes QCI 4	s5-uplnk-qci1totbyte
	Bytes QCI 5	s5-uplnk-qci1totbyte
	Bytes QCI 6	s5-uplnk-qci1totbyte
	Bytes QCI 7	s5-uplnk-qci1totbyte
	Bytes QCI 8	s5-uplnk-qci1totbyte
	Bytes QCI 9	s5-uplnk-qci1totbyte
	Bytes Non-Std QCI	s5-uplnk-othertotbyte
	Dropped Pkts QCI 1	s5-uplnk-drop-qci1totpkt
	Dropped Pkts QCI 2	s5-uplnk-drop-qci2totpkt
	Dropped Pkts QCI 3	s5-uplnk-drop-qci3totpkt
	Dropped Pkts QCI 4	s5-uplnk-drop-qci4totpkt
	Dropped Pkts QCI 5	s5-uplnk-drop-qci5totpkt
	Dropped Pkts QCI 6	s5-uplnk-drop-qci6totpkt
	Dropped Pkts QCI 7	s5-uplnk-drop-qci7totpkt
	Dropped Pkts QCI 8	s5-uplnk-drop-qci8totpkt
	Dropped Pkts QCI 9	s5-uplnk-drop-qci9totpkt
	Dropped Pkts Non-Std QCI	s5-uplnk-drop-otherpkt
	Dropped Bytes QCI 1	s5-uplnk-drop-qci1totbyte
	Dropped Bytes QCI 2	s5-uplnk-drop-qci2totbyte
	Dropped Bytes QCI 3	s5-uplnk-drop-qci3totbyte
	Dropped Bytes QCI 4	s5-uplnk-drop-qcir4totbyte
	Dropped Bytes QCI 5	s5-uplnk-drop-qci5totbyte
	Dropped Bytes QCI 6	s5-uplnk-drop-qci6totbyte
	Dropped Bytes QCI 7	s5-uplnk-drop-qci7totbyte
	Dropped Bytes QCI 8	s5-uplnk-drop-qci8totbyte
	Dropped Bytes QCI 9	s5-uplnk-drop-qci9totbyte
	Dropped Bytes Non-Std QCI	s5-uplnk-drop-othertotbyte
SGW Statistics / S5 Total Data Statistics / Downlink	Pkts	s5-downlnk-packets
	Bytes	s5-downlnk-bytes
	Dropped Pkts	s5-downlnk-dropped-packets
	Dropped Bytes	s5-downlnk-dropped-bytes

Table 4-7 SGW Bulk Statistic Enhancements in WEM Release 12.0

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
SGW Statistics / S5 Total Data Statistics / Downlink (con't.)	Pkts QCI 1	s5-downlnk-qci1totpkt
	Pkts QCI 2	s5-downlnk-qci2totpkt
	Pkts QCI 3	s5-downlnk-qci3totpkt
	Pkts QCI 4	s5-downlnk-qci4totpkt
	Pkts QCI 5	s5-downlnk-qci5otpkt
	Pkts QCI 6	s5-downlnk-qci6totpkt
	Pkts QCI 7	s5-downlnk-qci7totpkt
	Pkts QCI 8	s5-downlnk-qci8totpkt
	Pkts QCI 9	s5-downlnk-qci9totpkt
	Pkts Non-Std QCI	s5-downlnk-othertotpkt
	Bytes QCI 1	s5-downlnk-qci1totbyte
	Bytes QCI 2	s5-downlnk-qci2totbyte
	Bytes QCI 3	s5-downlnk-qci3totbyte
	Bytes QCI 4	s5-downlnk-qci4totbyte
	Bytes QCI 5	s5-downlnk-qci5totbyte
	Bytes QCI 6	s5-downlnk-qci6totbyte
	Bytes QCI 7	s5-downlnk-qci7totbyte
	Bytes QCI 8	s5-downlnk-qci8totbyte
	Bytes QCI 9	s5-downlnk-qci9totbyte
	Bytes Non-Std QCI	s5-downlnk-othertotbyte
	Dropped Pkts QCI 1	s5-downlnk-drop-qci1totpkt
	Dropped Pkts QCI 2	s5-downlnk-drop-qci2totpkt
	Dropped Pkts QCI 3	s5-downlnk-drop-qci3totpkt
	Dropped Pkts QCI 4	s5-downlnk-drop-qci4totpkt
	Dropped Pkts QCI 5	s5-downlnk-drop-qci5totpkt
	Dropped Pkts QCI 6	s5-downlnk-drop-qci6totpkt
	Dropped Pkts QCI 7	s5-downlnk-drop-qci7totpkt
	Dropped Pkts QCI 8	s5-downlnk-drop-qci8totpkt
	Dropped Pkts QCI 9	s5-downlnk-drop-qci9totpkt
	Dropped Pkts Non-Std QCI	s5-downlnk-drop-otherpkt
	Dropped Bytes QCI 1	s5-downlnk-drop-qci1totbyte
	Dropped Bytes QCI 2	s5-downlnk-drop-qci2totbyte
	Dropped Bytes QCI 3	s5-downlnk-drop-qci3totbyte
	Dropped Bytes QCI 4	s5-downlnk-drop-qci4totbyte
	Dropped Bytes QCI 5	s5-downlnk-drop-qci5totbyte
	Dropped Bytes QCI 6	s5-downlnk-drop-qci6totbyte
	Dropped Bytes QCI 7	s5-downlnk-drop-qci7totbyte
	Dropped Bytes QCI 8	s5-downlnk-drop-qci8totbyte
	Dropped Bytes QCI 9	s5-downlnk-drop-qci9totbyte

Table 4-7 SGW Bulk Statistic Enhancements in WEM Release 12.0

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
SGW Statistics / S5 Total Data Statistics / Downlink (con't.)	Dropped Bytes Non-Std QCI	s5-downlnk-drop-othertotbyte
	Dropped Pkts Non-Std QCI	s5-downlnk-drop-othertotpkt
SGW Statistics / S8 Total Data Statistics / Uplink	Pkts	s8-uplnk-packets
	Bytes	s8-uplnk-bytes
	Dropped Pkts	s8-uplnk-dropped-packets
	Dropped Bytes	s8-uplnk-dropped-bytes
	Pkts QCI 1	s8-uplnk-qci1totpkt
	Pkts QCI 2	s8-uplnk-qci2totpkt
	Pkts QCI 3	s8-uplnk-qci3totpkt
	Pkts QCI 4	s8-uplnk-qci4totpkt
	Pkts QCI 5	s8-uplnk-qci5totpkt
	Pkts QCI 6	s8-uplnk-qci6totpkt
	Pkts QCI 7	s8-uplnk-qci7totpkt
	Pkts QCI 8	s8-uplnk-qci8totpkt
	Pkts QCI 9	s8-uplnk-qci9totpkt
	Pkts Non-Std QCI	s8-uplnk-othertotpkt
	Bytes QCI 1	s8-uplnk-qci1totbyte
	Bytes QCI 2	s8-uplnk-qci1totbyte
	Bytes QCI 3	s8-uplnk-qci1totbyte
	Bytes QCI 4	s8-uplnk-qci1totbyte
	Bytes QCI 5	s8-uplnk-qci1totbyte
	Bytes QCI 6	s8-uplnk-qci1totbyte
	Bytes QCI 7	s8-uplnk-qci1totbyte
	Bytes QCI 8	s8-uplnk-qci1totbyte
	Bytes QCI 9	s8-uplnk-qci1totbyte
	Bytes Non-Std QCI	s8-uplnk-othertotbyte
	Dropped Pkts QCI 1	s8-uplnk-drop-qci1totpkt
	Dropped Pkts QCI 2	s8-uplnk-drop-qci2totpkt
	Dropped Pkts QCI 3	s8-uplnk-drop-qci3totpkt
	Dropped Pkts QCI 4	s8-uplnk-drop-qci4totpkt
	Dropped Pkts QCI 5	s8-uplnk-drop-qci5totpkt
	Dropped Pkts QCI 6	s8-uplnk-drop-qci6totpkt
	Dropped Pkts QCI 7	s8-uplnk-drop-qci7totpkt
	Dropped Pkts QCI 8	s8-uplnk-drop-qci8totpkt
	Dropped Pkts QCI 9	s8-uplnk-drop-qci9totpkt
	Dropped Pkts Non-Std QCI	s8-uplnk-drop-otherpkt
	Dropped Bytes QCI 1	s8-uplnk-drop-qci1totbyte
	Dropped Bytes QCI 2	s8-uplnk-drop-qci2totbyte
	Dropped Bytes QCI 3	s8-uplnk-drop-qci3totbyte
	Dropped Bytes QCI 4	s8-uplnk-drop-qcir4totbyte

Table 4-7 SGW Bulk Statistic Enhancements in WEM Release 12.0

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
SGW Statistics / S8 Total Data Statistics / Uplink (con't)	Dropped Bytes QCI 5	s8-uplnk-drop-qci5totbyte
	Dropped Bytes QCI 6	s8-uplnk-drop-qci6totbyte
	Dropped Bytes QCI 7	s8-uplnk-drop-qci7totbyte
	Dropped Bytes QCI 8	s8-uplnk-drop-qci8totbyte
	Dropped Bytes QCI 9	s8-uplnk-drop-qci9totbyte
	Dropped Bytes Non-Std QCI	s8-uplnk-drop-othertotbyte
SGW Statistics / S8 Total Data Statistics / Downlink	Pkts	s8-downlnk-packets
	Bytes	s8-downlnk-bytes
	Dropped Pkts	s8-downlnk-dropped-packets
	Dropped Bytes	s8-downlnk-dropped-bytes
	Pkts QCI 1	s8-downlnk-qci1totpkt
	Pkts QCI 2	s8-downlnk-qci2totpkt
	Pkts QCI 3	s8-downlnk-qci3totpkt
	Pkts QCI 4	s8-downlnk-qci4totpkt
	Pkts QCI 5	s8-downlnk-qci5otpkt
	Pkts QCI 6	s8-downlnk-qci6totpkt
	Pkts QCI 7	s8-downlnk-qci7totpkt
	Pkts QCI 8	s8-downlnk-qci8totpkt
	Pkts QCI 9	s8-downlnk-qci9totpkt
	Pkts Non-Std QCI	s8-downlnk-othertotpkt
	Bytes QCI 1	s8-downlnk-qci1totbyte
	Bytes QCI 2	s8-downlnk-qci2totbyte
	Bytes QCI 3	s8-downlnk-qci3totbyte
	Bytes QCI 4	s8-downlnk-qci4totbyte
	Bytes QCI 5	s8-downlnk-qci5totbyte
	Bytes QCI 6	s8-downlnk-qci6totbyte
	Bytes QCI 7	s8-downlnk-qci7totbyte
	Bytes QCI 8	s8-downlnk-qci8totbyte
	Bytes QCI 9	s8-downlnk-qci9totbyte
	Bytes Non-Std QCI	s8-downlnk-othertotbyte
	Dropped Pkts QCI 1	s8-downlnk-drop-qci1totpkt
	Dropped Pkts QCI 2	s8-downlnk-drop-qci2totpkt
	Dropped Pkts QCI 3	s8-downlnk-drop-qci3totpkt
	Dropped Pkts QCI 4	s8-downlnk-drop-qci4totpkt
	Dropped Pkts QCI 5	s8-downlnk-drop-qci5totpkt
	Dropped Pkts QCI 6	s8-downlnk-drop-qci6totpkt
	Dropped Pkts QCI 7	s8-downlnk-drop-qci7totpkt
	Dropped Pkts QCI 8	s8-downlnk-drop-qci8totpkt
	Dropped Pkts QCI 9	s8-downlnk-drop-qci9totpkt
	Dropped Pkts Non-Std QCI	s8-downlnk-drop-otherpkt

Table 4-7 SGW Bulk Statistic Enhancements in WEM Release 12.0

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
SGW Statistics / S8 Total Data Statistics / Downlink (count.)	Dropped Bytes QCI 1	s8-downlnk-drop-qci1totbyte
	Dropped Bytes QCI 2	s8-downlnk-drop-qci2totbyte
	Dropped Bytes QCI 3	s8-downlnk-drop-qci3totbyte
	Dropped Bytes QCI 4	s8-downlnk-drop-qci4totbyte
	Dropped Bytes QCI 5	s8-downlnk-drop-qci5totbyte
	Dropped Bytes QCI 6	s8-downlnk-drop-qci6totbyte
	Dropped Bytes QCI 7	s8-downlnk-drop-qci7totbyte
	Dropped Bytes QCI 8	s8-downlnk-drop-qci8totbyte
	Dropped Bytes QCI 9	s8-downlnk-drop-qci9totbyte
	Dropped Bytes Non-Std QCI	s8-downlnk-drop-othertotbyte
	Dropped Pkts Non-Std QCI	s8-downlnk-drop-othertotpkt
SGW Statistics / S5S8 Total Data Statistics / Uplink	Pkts	s5s8-uplnk-packets
	Bytes	s5s8-uplnk-bytes
	Dropped Pkts	s5s8-uplnk-dropped-packets
	Dropped Bytes	s5s8-uplnk-dropped-bytes
	Pkts QCI 1	s5s8-uplnk-qci1totpkt
	Pkts QCI 2	s5s8-uplnk-qci2totpkt
	Pkts QCI 3	s5s8-uplnk-qci3totpkt
	Pkts QCI 4	s5s8-uplnk-qci4totpkt
	Pkts QCI 5	s5s8-uplnk-qci5totpkt
	Pkts QCI 6	s5s8-uplnk-qci6totpkt
	Pkts QCI 7	s5s8-uplnk-qci7totpkt
	Pkts QCI 8	s5s8-uplnk-qci8totpkt
	Pkts QCI 9	s5s8-uplnk-qci9totpkt
	Pkts Non-Std QCI	s5s8-uplnk-othertotpkt
	Bytes QCI 1	s5s8-uplnk-qci1totbyte
	Bytes QCI 2	s5s8-uplnk-qci1totbyte
	Bytes QCI 3	s5s8-uplnk-qci1totbyte
	Bytes QCI 4	s5s8-uplnk-qci1totbyte
	Bytes QCI 5	s5s8-uplnk-qci1totbyte
	Bytes QCI 6	s5s8-uplnk-qci1totbyte
	Bytes QCI 7	s5s8-uplnk-qci1totbyte
	Bytes QCI 8	s5s8-uplnk-qci1totbyte
	Bytes QCI 9	s5s8-uplnk-qci1totbyte
	Bytes Non-Std QCI	s5s8-uplnk-othertotbyte
	Dropped Pkts QCI 1	s5s8-uplnk-drop-qci1totpkt
	Dropped Pkts QCI 2	s5s8-uplnk-drop-qci2totpkt
	Dropped Pkts QCI 3	s5s8-uplnk-drop-qci3totpkt
	Dropped Pkts QCI 4	s5s8-uplnk-drop-qci4totpkt
	Dropped Pkts QCI 5	s5s8-uplnk-drop-qci5totpkt

Table 4-7 SGW Bulk Statistic Enhancements in WEM Release 12.0

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
SGW Statistics / S5S8 Total Data Statistics / Uplink (con't)	Dropped Pkts QCI 6	s5s8-uplnk-drop-qci6totpkt
	Dropped Pkts QCI 7	s5s8-uplnk-drop-qci7totpkt
	Dropped Pkts QCI 8	s5s8-uplnk-drop-qci8totpkt
	Dropped Pkts QCI 9	s5s8-uplnk-drop-qci9totpkt
	Dropped Pkts Non-Std QCI	s5s8-uplnk-drop-otherpkt
	Dropped Bytes QCI 1	s5s8-uplnk-drop-qci1totbyte
	Dropped Bytes QCI 2	s5s8-uplnk-drop-qci2totbyte
	Dropped Bytes QCI 3	s5s8-uplnk-drop-qci3totbyte
	Dropped Bytes QCI 4	s5s8-uplnk-drop-qcir4totbyte
	Dropped Bytes QCI 5	s5s8-uplnk-drop-qci5totbyte
	Dropped Bytes QCI 6	s5s8-uplnk-drop-qci6totbyte
	Dropped Bytes QCI 7	s5s8-uplnk-drop-qci7totbyte
	Dropped Bytes QCI 8	s5s8-uplnk-drop-qci8totbyte
	Dropped Bytes QCI 9	s5s8-uplnk-drop-qci9totbyte
	Dropped Bytes Non-Std QCI	s5s8-uplnk-drop-othertotbyte
SGW Statistics / S5S8 Total Data Statistics / Downlink	Pkts	s5s8-downlnk-packets
	Bytes	s5s8-downlnk-bytes
	Dropped Pkts	s5s8-downlnk-dropped-packets
	Dropped Bytes	s5s8-downlnk-dropped-bytes
	Pkts QCI 1	s5s8-downlnk-qci1totpkt
	Pkts QCI 2	s5s8-downlnk-qci2totpkt
	Pkts QCI 3	s5s8-downlnk-qci3totpkt
	Pkts QCI 4	s5s8-downlnk-qci4totpkt
	Pkts QCI 5	s5s8-downlnk-qci5otpkt
	Pkts QCI 6	s5s8-downlnk-qci6totpkt
	Pkts QCI 7	s5s8-downlnk-qci7totpkt
	Pkts QCI 8	s5s8-downlnk-qci8totpkt
	Pkts QCI 9	s5s8-downlnk-qci9totpkt
	Pkts Non-Std QCI	s5s8-downlnk-othertotpkt
	Bytes QCI 1	s5s8-downlnk-qci1totbyte
	Bytes QCI 2	s5s8-downlnk-qci2totbyte
	Bytes QCI 3	s5s8-downlnk-qci3totbyte
	Bytes QCI 4	s5s8-downlnk-qci4totbyte
	Bytes QCI 5	s5s8-downlnk-qci5totbyte
	Bytes QCI 6	s5s8-downlnk-qci6totbyte
	Bytes QCI 7	s5s8-downlnk-qci7totbyte
	Bytes QCI 8	s5s8-downlnk-qci8totbyte
	Bytes QCI 9	s5s8-downlnk-qci9totbyte
	Bytes Non-Std QCI	s5s8-downlnk-othertotbyte
	Dropped Pkts QCI 1	s5s8-downlnk-drop-qci1totpkt

Table 4-7 SGW Bulk Statistic Enhancements in WEM Release 12.0

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
SGW Statistics / S5S8 Total Data Statistics / Downlink (con't)	Dropped Pkts QCI 2	s5s8-downlnk-drop-qci2totpkt
	Dropped Pkts QCI 3	s5s8-downlnk-drop-qci3totpkt
	Dropped Pkts QCI 4	s5s8-downlnk-drop-qci4totpkt
	Dropped Pkts QCI 5	s5s8-downlnk-drop-qci5totpkt
	Dropped Pkts QCI 6	s5s8-downlnk-drop-qci6totpkt
	Dropped Pkts QCI 7	s5s8-downlnk-drop-qci7totpkt
	Dropped Pkts QCI 8	s5s8-downlnk-drop-qci8totpkt
	Dropped Pkts QCI 9	s5s8-downlnk-drop-qci9totpkt
	Dropped Pkts Non-Std QCI	s5s8-downlnk-drop-otherpkt
	Dropped Bytes QCI 1	s5s8-downlnk-drop-qci1totbyte
	Dropped Bytes QCI 2	s5s8-downlnk-drop-qci2totbyte
	Dropped Bytes QCI 3	s5s8-downlnk-drop-qci3totbyte
	Dropped Bytes QCI 4	s5s8-downlnk-drop-qci4totbyte
	Dropped Bytes QCI 5	s5s8-downlnk-drop-qci5totbyte
	Dropped Bytes QCI 6	s5s8-downlnk-drop-qci6totbyte
	Dropped Bytes QCI 7	s5s8-downlnk-drop-qci7totbyte
	Dropped Bytes QCI 8	s5s8-downlnk-drop-qci8totbyte
	Dropped Bytes QCI 9	s5s8-downlnk-drop-qci9totbyte
	Dropped Bytes Non-Std QCI	s5s8-downlnk-drop-othertotbyte
	Dropped Pkts Non-Std QCI	s5s8-downlnk-drop-othertotpkt
SGW Statistics / S12 Total Data Statistics / Uplink	Pkts	s12-uplnk-packets
	Bytes	s12-uplnk-bytes
	Dropped Pkts	s12-uplnk-dropped-packets
	Dropped Bytes	s12-uplnk-dropped-bytes
	Pkts QCI 1	s12-uplnk-qci1totpkt
	Pkts QCI 2	s12-uplnk-qci2totpkt
	Pkts QCI 3	s12-uplnk-qci3totpkt
	Pkts QCI 4	s12-uplnk-qci4totpkt
	Pkts QCI 5	s12-uplnk-qci5totpkt
	Pkts QCI 6	s12-uplnk-qci6totpkt
	Pkts QCI 7	s12-uplnk-qci7totpkt
	Pkts QCI 8	s12-uplnk-qci8totpkt
	Pkts QCI 9	s12-uplnk-qci9totpkt
	Pkts Non-Std QCI	s12-uplnk-othertotpkt
	Bytes QCI 1	s12-uplnk-qci1totbyte
	Bytes QCI 2	s12-uplnk-qci1totbyte
	Bytes QCI 3	s12-uplnk-qci1totbyte
	Bytes QCI 4	s12-uplnk-qci1totbyte
	Bytes QCI 5	s12-uplnk-qci1totbyte

Table 4-7 SGW Bulk Statistic Enhancements in WEM Release 12.0

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
SGW Statistics / S12 Total Data Statistics / Uplink (con't)	Bytes QCI 6	s12-uplnk-qci1totbyte
	Bytes QCI 7	s12-uplnk-qci1totbyte
	Bytes QCI 8	s12-uplnk-qci1totbyte
	Bytes QCI 9	s12-uplnk-qci1totbyte
	Bytes Non-Std QCI	s12-uplnk-othertotbyte
	Dropped Pkts QCI 1	s12-uplnk-drop-qci1totpkt
	Dropped Pkts QCI 2	s12-uplnk-drop-qci2totpkt
	Dropped Pkts QCI 3	s12-uplnk-drop-qci3totpkt
	Dropped Pkts QCI 4	s12-uplnk-drop-qci4totpkt
	Dropped Pkts QCI 5	s12-uplnk-drop-qci5totpkt
	Dropped Pkts QCI 6	s12-uplnk-drop-qci6totpkt
	Dropped Pkts QCI 7	s12-uplnk-drop-qci7totpkt
	Dropped Pkts QCI 8	s12-uplnk-drop-qci8totpkt
	Dropped Pkts QCI 9	s12-uplnk-drop-qci9totpkt
	Dropped Pkts Non-Std QCI	s12-uplnk-drop-otherpkt
	Dropped Bytes QCI 1	s12-uplnk-drop-qci1totbyte
	Dropped Bytes QCI 2	s12-uplnk-drop-qci2totbyte
	Dropped Bytes QCI 3	s12-uplnk-drop-qci3totbyte
	Dropped Bytes QCI 4	s12-uplnk-drop-qcir4totbyte
	Dropped Bytes QCI 5	s12-uplnk-drop-qci5totbyte
	Dropped Bytes QCI 6	s12-uplnk-drop-qci6totbyte
	Dropped Bytes QCI 7	s12-uplnk-drop-qci7totbyte
	Dropped Bytes QCI 8	s12-uplnk-drop-qci8totbyte
	Dropped Bytes QCI 9	s12-uplnk-drop-qci9totbyte
	Dropped Bytes Non-Std QCI	s12-uplnk-drop-othertotbyte
SGW Statistics / S12 Total Data Statistics / Downlink	Pkts	s12-downlnk-packets
	Bytes	s12-downlnk-bytes
	Dropped Pkts	s12-downlnk-dropped-packets
	Dropped Bytes	s12-downlnk-dropped-bytes
	Pkts QCI 1	s12-downlnk-qci1totpkt
	Pkts QCI 2	s12-downlnk-qci2totpkt
	Pkts QCI 3	s12-downlnk-qci3totpkt
	Pkts QCI 4	s12-downlnk-qci4totpkt
	Pkts QCI 5	s12-downlnk-qci5otpkt
	Pkts QCI 6	s12-downlnk-qci6totpkt
	Pkts QCI 7	s12-downlnk-qci7totpkt
	Pkts QCI 8	s12-downlnk-qci8totpkt
	Pkts QCI 9	s12-downlnk-qci9totpkt
	Pkts Non-Std QCI	s12-downlnk-othertotpkt

Table 4-7 SGW Bulk Statistic Enhancements in WEM Release 12.0

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
SGW Statistics / S12 Total Data Statistics / Downlink (con't)	Bytes QCI 1	s12-downlnk-qci1totbyte
	Bytes QCI 2	s12-downlnk-qci2totbyte
	Bytes QCI 3	s12-downlnk-qci3totbyte
	Bytes QCI 4	s12-downlnk-qci4totbyte
	Bytes QCI 5	s12-downlnk-qci5totbyte
	Bytes QCI 6	s12-downlnk-qci6totbyte
	Bytes QCI 7	s12-downlnk-qci7totbyte
	Bytes QCI 8	s12-downlnk-qci8totbyte
	Bytes QCI 9	s12-downlnk-qci9totbyte
	Bytes Non-Std QCI	s12-downlnk-othertotbyte
	Dropped Pkts QCI 1	s12-downlnk-drop-qci1totpkt
	Dropped Pkts QCI 2	s12-downlnk-drop-qci2totpkt
	Dropped Pkts QCI 3	s12-downlnk-drop-qci3totpkt
	Dropped Pkts QCI 4	s12-downlnk-drop-qci4totpkt
	Dropped Pkts QCI 5	s12-downlnk-drop-qci5totpkt
	Dropped Pkts QCI 6	s12-downlnk-drop-qci6totpkt
	Dropped Pkts QCI 7	s12-downlnk-drop-qci7totpkt
	Dropped Pkts QCI 8	s12-downlnk-drop-qci8totpkt
	Dropped Pkts QCI 9	s12-downlnk-drop-qci9totpkt
	Dropped Pkts Non-Std QCI	s12-downlnk-drop-otherpkt
	Dropped Bytes QCI 1	s12-downlnk-drop-qci1totbyte
	Dropped Bytes QCI 2	s12-downlnk-drop-qci2totbyte
	Dropped Bytes QCI 3	s12-downlnk-drop-qci3totbyte
	Dropped Bytes QCI 4	s12-downlnk-drop-qci4totbyte
	Dropped Bytes QCI 5	s12-downlnk-drop-qci5totbyte
	Dropped Bytes QCI 6	s12-downlnk-drop-qci6totbyte
	Dropped Bytes QCI 7	s12-downlnk-drop-qci7totbyte
	Dropped Bytes QCI 8	s12-downlnk-drop-qci8totbyte
	Dropped Bytes QCI 9	s12-downlnk-drop-qci9totbyte
	Dropped Bytes Non-Std QCI	s12-downlnk-drop-othertotbyte
	Dropped Pkts Non-Std QCI	s12-downlnk-drop-othertotpkt

Web Element Manager Path

- Accounting | Bulk Statistics Configuration | Schema Tab
- Accounting | View/Graph Bulk Statistics | Select Counters and Filters Parameters Tab

ECS Bulk Statistic Enhancements

The following bulk statistics were added to the ECS schema in WEM Release 12.0.

Table 4-8 ECS Bulk Statistic Enhancements in WEM Release 12.0

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
ECS Statistics / TFTP	Total TFTP Flows	tftp-flows
	Total Uplink Bytes	tftp-uplk-bytes
	Total Uplink Packets	tftp-uplk-pkts
	Total Downlink Bytes	tftp-dwnlk-bytes
	Total Downlink Packets	tftp-dwnlk-pkts
	Total Read Sessions	tftp-total-read-sessions
	Total Write Sessions	tftp-total-write-sessions
	Total Packets with Unknown Request Type	tftp-unsupp-req-pkts
	Total Invalid Control Packets	tftp-invalid-ctrl-pkts
	Total Invalid Data Packets	tftp-invalid-data-pkts
	Uplink Data Bytes	tftp-data-uplk-bytes
	Downlink Data Bytes	tftp-data-dwnlk-bytes
	Uplink Data Pkts	tftp-data-uplk-pkts
	Downlink Data Pkts	tftp-data-dwnlk-pkts

Web Element Manager Path

- Accounting | Bulk Statistics Configuration | Schema Tab
- Accounting | View/Graph Bulk Statistics | Select Counters and Filters Parameters Tab

Changes in Data Values to HNBGW SCTP Schema Bulk Statistics

The following HNBGW SCTP bulk statistics data values have been changed from Int32 to **Int64** to accommodate the potential value of the statistics.

Table 4-9 HNBGW SCTP Bulk Statistic Schema Data Values Changed to Int64 in WEM Release 12.0

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
HNBGW SCTP Statistics / SCTP	Total Bytes Sent To Lower Layer	total-bytes-sent-to-lower-layer
	Total Bytes Received From Lower Layer	total-bytes-rcvd-from-lower-layer
	Total Packets Sent To Lower Layer	total-packets-sent-to-lower-layer
	Total Packets Received From Lower Layer	total-packets-rcvd-from-lower-layer
HNBGW SCTP Statistics / SCTP / Transmitted SCTP Data	Init Chunks	trans-sctp-data-init-chunks
	Init Ack Chunks	trans-sctp-data-init-ack-chunks
	Shutdown Chunks	trans-sctp-data-shutdown-chunks
	Shutdown Ack Chunks	trans-sctp-data-shutdown-ack-chunks
	Cookie Chunks	trans-sctp-data-cookie-chunks
	Cookie Ack Chunks	trans-sctp-data-cookie-ack-chunks
	Data Chunks	trans-sctp-data-data-chunks
	Data Ack Chunks	trans-sctp-data-data-ack-chunks
	Shutdown Complete Chunks	trans-sctp-data-shutdown-comp-chunks

Table 4-9 HNBGW SCTP Bulk Statistic Schema Data Values Changed to Int64 in WEM Release 12.0

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
HNBGW SCTP Statistics / SCTP / Transmitted SCTP Data (con't)	Heartbeat Chunks	trans-sctp-data-heartbeat-chunks
	HeartBeat Ack Chunks	trans-sctp-data-heartbeat-chunks
	Abort Chunks	trans-sctp-data-abort-chunks
	Error Chunks	trans-sctp-data-error-chunks
HNBGW SCTP Statistics / Received SCTP Data	Init Chunks	rcvd-sctp-data-init-chunks
	Init Ack Chunks	rcvd-sctp-data-init-ack-chunks
	Shutdown Chunks	rcvd-sctp-data-shutdown-chunks
	Shutdown Ack Chunks	rcvd-sctp-data-shutdown-ack-chunks
	Cookie Chunks	rcvd-sctp-data-cookie-chunks
	Cookie Ack Chunks	rcvd-sctp-data-cookie-ack-chunks
	Data Chunks	rcvd-sctp-data-data-chunks
	Data Ack Chunks	rcvd-sctp-data-data-chunks
	Shutdown Complete Chunks	rcvd-sctp-data-shutdown-comp-chunks
	Heartbeat Chunks	rcvd-sctp-data-heartbeat-chunks
	HeartBeat Ack Chunks	rcvd-sctp-data-heartbeat-ack-chunks
	Abort Chunks	rcvd-sctp-data-abort-chunks
	Error Chunks	rcvd-sctp-data-error-chunks
HNBGW SCTP Statistics / Retransmitted SCTP Data	Init Chunks	retrans-sctp-data-init-chunks
	Shutdown Chunks	retrans-sctp-data-shutdown-chunks
	Shutdown Ack Chunks	retrans-sctp-data-shutdown-ack-chunks
	Data Chunks	retrans-sctp-data-data-chunks
	Cookie Chunks	retrans-sctp-data-cookie-chunks

Web Element Manager Path

On the WEM server: <*ems_dir*>/server/bsschema/hnbgw_sctp_counter.xml

Changes in Data Values to HNBGW RTP Schema Bulk Statistics

The following HNBGW RTP bulk statistics data values have been changed from Int32 to **Int64** to accommodate the potential value of the statistics.

Table 4-10 HNBGW RTP Bulk Statistic Schema Data Values Changed to Int64 in WEM Release 12.0

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
HNBGW RTP Statistics / RTP	RTP Uplink Packets Rx	rtp-uplink-pkts-rx
	RTP Uplink Bytes Rx	rtp-uplink-byts-rx
	RTP Uplink Packets dropped	rtp-uplink-pkts-dropped
	RTP Uplink Bytes dropped	rtp-uplink-byts-dropped
	RTP Downlink Packets Tx	rtp-downlink-pkts-tx
	RTP Downlink Bytes Tx	rtp-downlink-byts-tx

Table 4-10 HNBGW RTP Bulk Statistic Schema Data Values Changed to Int64 in WEM Release 12.0

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
HNBGW RTP Statistics / RTP / RTP Uplink Packets Drop Cause	RAB not in CONNECTED state	rtp-uplink-pkts-drop-rab_not-in_conn_state
	Miscellaneous	rtp-uplink-pkts-dropped-misc
HNBGW RTP Statistics / RTP / RTP Uplink Bytes Drop Cause	RAB not in CONNECTED state	rtp-uplink-byts-drop-rab_not-in_conn_state
	Miscellaneous	rtp-uplink-byts-dropped-misc
HNBGW RTP Statistics / RTP / RTCP	Sender Report Rx (From HNB)	rtcp-sender-report-rx
	RTCP Sender Report Tx (To HNB)	rtcp-sender-report-tx
	RTCP SDES Report Rx (From HNB)	rtcp-sdes-report-rx
	RTCP SDES Report Tx (To HNB)	rtcp-sdes-report-tx
	RTCP BYE Report Rx (From HNB)	rtcp-bye-report-rx
	RTCP APP Report Tx (From HNB)	rtcp-app-report-rx
	RTCP Uplink Packets Rx	rtcp-uplink-pkts-rx
	RTCP Uplink Bytes Rx	rtcp-uplink-byts-rx
	RTCP Uplink Packets dropped	rtcp-uplink-pkts-dropped
	RTCP Uplink Bytes dropped	rtcp-uplink-pkts-dropped
	RTCP Downlink Packets Tx	rtcp-downlink-pkts-tx
	RTCP Downlink Bytes Tx	rtcp-downlink-byts-tx
HNBGW RTP Statistics / RTP / RTCP / Uplink Packets Drop Cause	RAB not in CONNECTED state	rtcp-uplink-pkts-drop-rab_not-in_conn_stat e
	Miscellaneous	rtcp-uplink-pkts-dropped-misc
HNBGW RTP Statistics / RTP-MUX	RTP-MUX Uplink Packets Rx	rtp-mux-uplink-pkts-rx
	RTP-MUX Uplink Packets dropped	rtp-mux-uplink-pkts-dropped
	RTP-MUX Uplink Bytes Rx	rtp-mux-uplink-byts-rx
	RTP-MUX Uplink Bytes dropped	rtp-mux-uplink-byts-dropped
	RTP-MUX RTP Stream Received	rtp-mux-rtp-stream-rcvd
	RTP-MUX RTP Stream Dropped	rtp-mux-rtp-stream-dropped
HNBGW RTP Statistics / RTP-MUX / RTP-MUX Uplink Packets Drop Cause	Miscellaneous	rtp-mux-uplink-pkts-dropped-misc
HNBGW RTP Statistics / RTP-MUX / RTP-MUX Uplink Bytes Drop Cause	Miscellaneous	rtp-mux-uplink-byts-dropped-misc
HNBGW RTP Statistics / RTP-MUX / RTP-MUX Stream Drop Cause	Miscellaneous	rtp-mux-rtp-stream-dropped-misc

Web Element Manager Path

On the WEM server: <*ems_dir*>/server/bsschema/hnbgw_rtp_counter.xml.

Changes in Data Values to CS NW RTP Schema Bulk Statistics

The following CS NW RTP bulk statistics data values have been changed from Int32 to **Int64** to accommodate the potential value of the statistics.

Table 4-11 CS NW RTP Schema Bulk Statistics Data Values Changed to Int64 in WEM Release 12.0

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
CS NW RTP Statistics / RTP	RTP Uplink Packets Tx	rtp-uplink-pkts-tx
	RTP Uplink Bytes Tx	rtp-uplink-byts-tx
	RTP Downlink Packets Rx	rtp-downlink-pkts-rx
	RTP Downlink Bytes Rx	rtp-downlink-byts-rx
	RTP Downlink Packets dropped	rtp-downlink-pkts-dropped
	RTP Downlink Bytes dropped	rtp-downlink-byts-dropped
CS NW RTP Statistics / RTP / Downlink Packets Drop Cause	RAB not in CONNECTED state	rtp-downlink-pkts-drop-rab_not-in_conn_state
	Miscellaneous	rtp-downlink-pkts-drop-misc
CS NW RTP Statistics / RTP / Downlink Bytes Drop Cause	RAB not in CONNETED state	rtp-downlink-byts-drop-rab_not-in_conn_state
	Miscellaneous	rtp-downlink-byts-drop-misc
CS NW RTP Statistics / RTPC	RTCP Uplink Packets Tx	rtcp-uplink-pkts-tx
	RTCP Uplink Bytes Tx	rtcp-uplink-byts-tx
	RTCP Downlink Packets Rx	rtcp-downlink-pkts-rx
	RTCP Downlink Bytes Rx	rtcp-downlink-byts-rx
	RTCP Downlink Packets dropped	rtcp-downlink-pkts-dropped
	RTCP Downlink Bytes dropped	rtcp-downlink-byts-dropped
CS NW RTP Statistics / RTPC / RTPC Downlink Packets Drop Cause	RAB not in CONNECTED state	rtcp-downlink-pkts-drop-rab_not-in_conn_state
	Miscellaneous	rtcp-downlink-pkts-drop-misc
CS NW RTP Statistics / RTPC / RTPC Downlink Bytes Drop Cause	RAB not in CONNECTED state	rtcp-downlink-byts-drop-rab_not-in_conn_state
	Miscellaneous	rtcp-downlink-byts-drop-misc

Web Element Manager Path

On the WEM server: <*ems_dir*>/server/bsschema/cs_nw_rtp_counter.xml

Changes in Data Values to AAL2 Schema Bulk Statistics

The following AAL2 bulk statistics data values have been changed from Int32 to **Int64** to accommodate the potential value of the statistics.

Table 4-12 AAL2 Bulk Statistic Schema Values Changed to Data Value Int64 in WEM Release 12.0

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
AAL2 Statistics / AAL2	AAL2 Uplink Packets Tx	uplink-pkts-tx
	AAL2 Uplink Bytes Tx	uplink-byts-tx
	AAL2 Downlink Packets Rx	downlink-pkts-rx
	AAL2 Downlink Bytes Rx	downlink-byts-rx
	AAL2 Downlink Packets dropped	downlink-pkts-dropped
	AAL2 Downlink Bytes dropped	downlink-byts-dropped

Table 4-12 AAL2 Bulk Statistic Schema Values Changed to Data Value Int64 in WEM Release 12.0

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
AAL2 Statistics / AAL2 / AAL2 Downlink Packets Drop Cause	RAB not in CONNECTED state	downlink-pkts-drop-rab-not-in-conn-state
	Miscellaneous	downlink-pkts-drop-cause-misc
AAL2 Statistics / AAL2 / AAL2 Downlink Bytes Drop Cause	RAB not in CONNECTED state	downlink-byts-drop-rab-not-in-conn-state
	Miscellaneous	downlink-byts-drop-cause-misc

Web Element Manager Path

On the WEM server: <*ems_dir*>/server/bsschema/aal2_counter.xml

Changes in Data Values to MME Schema Bulk Statistics

The following mme bulk statistics data values have been changed from Incremental to Gauge.

Table 4-13 MME Bulk Statistic Schema Values Changed to Gauge in WEM Release 12.0

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
MME Statistics	Attached Calls	emmcall-attach-currcall
	Maximum Calls	emmcall-attach-maxcall
	Current Calls	emmcall-connect-curcall
	Maximum Calls	emmcall-connect-maxcall
	Current Calls	emmcall-idle-curcall
	Maximum Calls	emmcall-idle-maxcall

Web Element Manager Path

On the WEM server: <*ems_dir*>/server/bsschema/mme_counter.xml

New Bulkstatistic Schemas

The following Schemas can be found in the XML files on the WEM server:

- ENAPP
- Misc_for_EMS
- PDG
- PROFAPP
- SHAPP

Web Element Manager Path

On the WEM server: <*ems_dir*>/server/bsschema/<*schema name*>

For counter descriptions, refer to the latest edition of the *Statistics and Counters Reference*.

Web Element Manager Accounting Enhancements in Release 12.2

The following WEM Accounting enhancements were made for Release 12.2.

Enhancements to View/Graph Bulk Statistics Feature

Previously, the Bulk Statistics Graphing feature allowed the user to view only 20 data sample points per page. This required the user to click to a second page if the number of data points exceeded 20.

The Bulk Statistics Graphing feature has been enhanced to allow the user to zoom in or out to view as few or as many graph data samplings on a single page. By providing a zoom a mechanism for viewing a large number of data samples on a single screen, users can more effective analyze the trend shown in the graph.

The slider mechanism is just below the graph display. By moving the slider control to the left or right, the user can decrease or increase the number of data samples shown.

Above the graph display, there are discrete zoom controls that allow the user to click to see one of the following graph views:

- 1hr: Display all data samples for a one-hour period.
- 3hr: Display all data samples for a three-hour period.
- 6hr: Display all data samples for a six-hour period.
- Max: Display all available data samples

IMPORTANT

The existing X-scale, X-scroll and Y-scale functionality have been replaced by the zoom in/zoom out feature. In addition, the Page size label has been removed, as the new zoom feature eliminates the need to view a graph over multiple pages.

Web Element Manager Path

- Accounting | View/Graph Bulk Statistics

GTPC Bulk Statistic Schema Support

GTPC schema bulk statistics support is now available in WEM.

Web Element Manager Path

Accounting Menu | Bulk Statistics Configuration | Bulk Statistics Dialog Box | Bulk Statistics Configuration Dialog Box - Schema Tab

System Schema Bulk Statistic Enhancements

The following bulk statistics have been added to the System schema in WEM Release 12.2.

Table 4-14 System Bulk Statistic Enhancements in WEM Release 12.2

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
System Schema / ASNGW Managers	Service Flow Information	asngw-sfs
	TID Failures	asngw-tidfail
System Schema / Session Disconnect Reasons	sgsn-egtpc-connection-failed	disc-reason-438
	sgsn-egtpc-create-session-failed	disc-reason-439
	sgsn-hss-detach	disc-reason-440
	sgsn-hss-connection-failure	disc-reason-441
	sgsn-pgw-detach	disc-reason-442
	sgsn-s5-not-supported-for-apn	disc-reason-443
	sgsn-no-rab-for-gbr-bearer	disc-reason-444
	sgsn-sgw-selection-failure	disc-reason-445
	sgsn-pgw-selection-failure	disc-reason-446
	wimax-hotlining-status-change	disc-reason-447
	ggsn-no-rsp-from-sgsn	disc-reason-448
	diameter-protocol-error	disc-reason-449
	diameter-request-timeout	disc-reason-450
	operator-policy	disc-reason-451
	spr-connection-error	disc-reason-452
	mipha-dup-wimax-session	disc-reason-453
	invalid-version-attr	disc-reason-454
	sgsn-zone-code-failure	disc-reason-455/
	invalid-qci	disc-reason-456
	no_rules	disc-reason-457
	sgsn-rnc-no-dual-pdp-init-pdp-deact	disc-reason-458
	mme-init-ctxt-setup-failure	disc-reason-459

Table 4-14 System Bulk Statistic Enhancements in WEM Release 12.2

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
System Schema / Session Disconnect Reasons (con't)	mme-driver-initiated	disc-reason-460
	mme-s1ap-connection-down	disc-reason-461
	mme-s1ap-reset-recd	disc-reason-462
	mme-s6a-response-timeout	disc-reason-463
	mme-s13-response-timeout	disc-reason-464
	mme-Illegal-equipment	disc-reason-465
	mme-unexpected-attach	disc-reason-466
	mme-sgw-selection-failure	disc-reason-467
	mme-pgw-selection-failure	disc-reason-468
	mme-reselection-to-sgsn	disc-reason-469
	mme-relocation-to-sgsn	disc-reason-470
	mme-reselection-to-mm	disc-reason-471
	mme-relocation-to-mme	disc-reason-472
	mme-tau-attach-collision	disc-reason-473
	mme-old-sgsn-resolution-failure	disc-reason-474
	mme-old-mme-resolution-failure	disc-reason-475
	mme-reloc-ho-notify-timeout	disc-reason-476
	mme-reloc-ho-req-ack-timeout	disc-reason-477
	mme-create-session-timeout	disc-reason-478
	mme-create-session-failure	disc-reason-479
	mme-s11-path-failure	disc-reason-480
	mme-policy-no-ue-irat	disc-reason-481
	mme-x2-handover-failed	disc-reason-482
	mme-attach-restrict	disc-reason-483
	mme-regional-zone-code	disc-reason-484
	mme-no-response-from-ue	disc-reason-485
	mme-sgw-relocation-failed	disc-reason-486
	mme-implicit-detach	disc-reason-487
	sgsn-detach-notify	disc-reason-488
	emergency-inactivity-timeout	disc-reason-489
	policy-initiated-release	disc-reason-490
	gy-result-code-system-failure	disc-reason-491
	mme-zone-code-validation-failed	disc-reason-492
System Statistics / CC Update Reporting Reason Statistics	TITSU Time	cc-upd-titsutime
System Statistics / CCA Initial Message Stats	Result Code 2001	cca-init-2001-rc
	Result Code 4011	cca-init-4011-rc
	Result Code 4012	cca-init-4012-rc
	Result Code 5003	cca-init-5003-rc

Table 4-14 System Bulk Statistic Enhancements in WEM Release 12.2

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
System Statistics / CCA Update Message Stats	Result Code 2001	cca-updt-2001-rc
	Result Code 4011	cca-updt-4011-rc
	Result Code 4012	cca-updt-4012-rc
	Result Code 5003	cca-updt-5003-rc
System Statistics / Failure Handling Stats	Action-Continue	fail-action-contd
	Action-Terminated	fail-action-term
System Statistics / Miscellaneous	NPU Flow - Usage	npu-capacity-usage
	NPU Flow - Effective	npu-capacity
	Session Information - Capacity Usage	session-capacity-usage
	System Capacity Usage	system-capacity-usage
	Session Information - Capacity	session-capacity
System Statistics / Number of Active Sessions	PDSN	pdsn-activdata
	HSGW	hsgw-activdata
	ASNGW	asngw-activdata
	HA	ha-activedata
	MME	mme-activedata
	PGW	pgw-activedata
	SGW	sgw-activedata
System Statistics / LTE Node Tunnels Statistics	Total IPsec Manager Death Notifications	ipsecctrl-lte-ipsecmgr-death-notif
	Total Crypto Maps Delete Requests	ipsecctrl-lte-map-del-reqs
	Total Crypto Maps Established	ipsecctrl-lte-map-est
	Total Crypto Maps Failed	ipsecctrl-lte-map-failed
	Total Crypto Map Requests	ipsecctrl-lte-map-reqs
	Total Crypto Maps State Change Notifications Sent	ipsecctrl-lte-map-state-notif
	Total Crypto Maps with QoS	ipsecctrl-lte-qos-maps
	Total Service Template Requests	ipsecctrl-lte-template-reqs
	Total Service Template Unregister Requests	ipsecctrl-lte-template-unreg-reqs

Web Element Manager Path

- Accounting | Bulk Statistics Configuration | Schema Tab
- Accounting | View/Graph Bulk Statistics | Select Counters and Filters Parameters Tab

SGW Schema Bulk Statistic Enhancements

The following bulk statistics have been added to the SGW schema in WEM Release 12.2.

Table 4-15 SGW Bulk Statistic Enhancements in WEM Release 12.2

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
SGW Statistics / S1U Total Data Statistics / Downlink	Dropped Bytes Non-Std QCI	datastat-downlink-dropstat-othertotbyte
	Dropped Pkts Non-Std QCI	datastat-downlink-dropstat-othertotpkt
	Dropped Bytes QCI1	datastat-downlink-dropstat-qci1totbyte
	Dropped Pkts QCI1	datastat-downlink-dropstat-qci1totpkt
	Dropped Bytes QCI2	datastat-downlink-dropstat-qci2totbyte
	Dropped Pkts QCI2	datastat-downlink-dropstat-qci2totpkt
	Dropped Bytes QCI3	datastat-downlink-dropstat-qci3totbyte
	Dropped Pkts QCI3	datastat-downlink-dropstat-qci3totpkt
	Dropped Bytes QCI4	datastat-downlink-dropstat-qci4totbyte
	Dropped Pkts QCI4	datastat-downlink-dropstat-qci4totpkt
	Dropped Bytes QCI5	datastat-downlink-dropstat-qci5totbyte
	Dropped Pkts QCI5	datastat-downlink-dropstat-qci5totpkt
	Dropped Bytes QCI6	datastat-downlink-dropstat-qci6totbyte
	Dropped Pkts QCI6	datastat-downlink-dropstat-qci6totpkt
	Dropped Bytes QCI7	datastat-downlink-dropstat-qci7totbyte
	Dropped Pkts QCI7	datastat-downlink-dropstat-qci7totpkt
	Dropped Bytes QCI8	datastat-downlink-dropstat-qci8totbyte
	Dropped Pkts QCI8	datastat-downlink-dropstat-qci8totpkt
	Dropped Bytes QCI9	datastat-downlink-dropstat-qci9totbyte
	Dropped Pkts QCI9	datastat-downlink-dropstat-qci9totpkt
	Bytes Non-Std QCI	datastat-downlink-othertotbyte
	Pkts Non-Std QCI	datastat-downlink-othertotpkt
	Bytes QCI 1	datastat-downlink-qci1totbyte
	Pkts QCI 1	datastat-downlink-qci1totpkt
	Bytes QCI 2	datastat-downlink-qci2totbyte
	Pkts QCI 2	datastat-downlink-qci2totpkt
	Bytes QCI 3	datastat-downlink-qci3totbyte
	Pkts QCI 3	datastat-downlink-qci3totpkt
	Bytes QCI 4	datastat-downlink-qci4totbyte
	Pkts QCI 4	datastat-downlink-qci4totpkt
	Bytes QCI 5	datastat-downlink-qci5totbyte
	Pkts QCI 5	datastat-downlink-qci5totpkt
	Bytes QCI 6	datastat-downlink-qci6totbyte
	Pkts QCI 6	datastat-downlink-qci6totpkt
	Bytes QCI 7	datastat-downlink-qci7totbyte
	Pkts QCI 7	datastat-downlink-qci7totpkt
	Bytes QCI 8	datastat-downlink-qci8totbyte
	Pkts QCI 8	datastat-downlink-qci8totpkt

Table 4-15 SGW Bulk Statistic Enhancements in WEM Release 12.2

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
SGW Statistics / S1U Total Data Statistics / Downlink (con't)	Bytes QCI 9	datastat-downlink-qci9totbyte
	Pkts QCI 9	datastat-downlink-qci9totpkt
	Dropped Pkts Non-Std QCI	s1u-downlnk-drop-othertotpkt
SGW Statistics / S1U Total Data Statistics / Uplink	Pkts Non-Std QCI	datastat-uplink-dropstat-othertotpkt
	Dropped Bytes QCI 1	datastat-uplink-dropstat-qci1totbyte
	Dropped Pkts QCI 1	datastat-uplink-dropstat-qci1totpkt
	Dropped Bytes QCI 2	datastat-uplink-dropstat-qci2totbyte
	Dropped Pkts QCI 2	datastat-uplink-dropstat-qci2totpkt
	Dropped Bytes QCI 3	datastat-uplink-dropstat-qci3totbyte
	Dropped Pkts QCI 3	datastat-uplink-dropstat-qci3totpkt
	Dropped Bytes QCI 4	datastat-uplink-dropstat-qci4totbyte
	Dropped Pkts QCI 4	datastat-uplink-dropstat-qci4totpkt
	Dropped Bytes QCI 5	datastat-uplink-dropstat-qci5totbyte
	Dropped Pkts QCI 5	datastat-uplink-dropstat-qci5totpkt
	Dropped Bytes QCI 6	datastat-uplink-dropstat-qci6totbyte
	Dropped Pkts QCI 6	datastat-uplink-dropstat-qci6totpkt
	Dropped Bytes QCI 7	datastat-uplink-dropstat-qci7totbyte
	Dropped Pkts QCI 7	datastat-uplink-dropstat-qci7totpkt
	Dropped Bytes QCI 8	datastat-uplink-dropstat-qci8totbyte
	Dropped Pkts QCI 8	datastat-uplink-dropstat-qci8totpkt
	Dropped Bytes QCI 9	datastat-uplink-dropstat-qci9totbyte
	Dropped Pkts QCI 9	datastat-uplink-dropstat-qci9totpkt
	Bytes Non-Std QCI	datastat-uplink-othertotbyte
	Pkts Non-Std QCI	datastat-uplink-othertotpkt
	Bytes QCI 1	datastat-uplink-qci1totbyte
	Pkts QCI 1	datastat-uplink-qci1totpkt
	Bytes QCI 2	datastat-uplink-qci2totbyte
	Pkts QCI 2	datastat-uplink-qci2totpkt
	Bytes QCI 3	datastat-uplink-qci3totbyte
	Pkts QCI 3	datastat-uplink-qci3totpkt
	Bytes QCI 4	datastat-uplink-qci4totbyte
	Pkts QCI 4	datastat-uplink-qci4totpkt
	Bytes QCI 5	datastat-uplink-qci5totbyte
	Pkts QCI 5	datastat-uplink-qci5totpkt
	Bytes QCI 6	datastat-uplink-qci6totbyte
	Pkts QCI 6	datastat-uplink-qci6totpkt
	Bytes QCI 7	datastat-uplink-qci7totbyte

Table 4-15 SGW Bulk Statistic Enhancements in WEM Release 12.2

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
SGW Statistics / S1U Total Data Statistics / Uplink (con't)	Pkts QCI 7	datastat-uplink-qci7totpkt
	Bytes QCI 8	datastat-uplink-qci8totbyte
	Pkts QCI 8	datastat-uplink-qci8totpkt
	Bytes QCI 9	datastat-uplink-qci9totbyte
	Pkts QCI 9	datastat-uplink-qci9totpkt
SGW Statistics / S1U Total Data Statistics / Intra-SGW Handover Statistics	Intra-MME	intrasgwhaovstat-intramme
	Inter-MME	intrasgwhaovstat-intermme
SGW Statistics / Inter-SGW Handover Statistics / Inter System	Inter System (directory)	intersgwhaovstat-intersystem
	Success	intersgwhaovstat-intersystem-success
	Fail	intersgwhaovstat-intersystem-fail
SGW Statistics / Intra-SGW Handover Statistics	Inter-MME (directory)	intrasgwhaovstat-intermme
	Success	intrasgwhaovstat-intermme-success
	Fail	intrasgwhaovstat-intermme-fail
	Intra-MME (directory)	intrasgwhaovstat-intramme
	Success	intrasgwhaovstat-intramme-success
	Fail	intrasgwhaovstat-intramme-fail
SGW Statistics / PDN PLM Statistics / Home PDNs	PDNs active	plmnstat-home-pdn-active
	PDNs released	plmnstat-home-pdn-released
	PDNs setup	plmnstat-home-pdn-setup
SGW Statistics / PDN PLM Statistics / Roaming PDNs	PDNs active	plmnstat-roam-pdn-active
	PDNs setup	plmnstat-roam-pdn-setup
	PDNs released	plmnstat-roam-pdn-released
SGW Statistics / PDN PLM Statistics / Visiting PDNs	PDNs active	plmnstat-vist-pdn-active
	PDNs setup	plmnstat-vist-pdn-setup
	PDNs released	plmnstat-vist-pdn-released
SGW Statistics / S12 Total Data Statistics / Downlink	Dropped Pkts Non-Std QCI	s12-downlnk-drop-othertotpkt
SGW Statistics / S4U Total Data Statistics / Downlink	Dropped Pkts Non-Std QCI	s4u-downlnk-drop-othertotpkt
SGW Statistics / S5 Total Data Statistics / Downlink	Dropped Pkts Non-Std QCI	s5-downlnk-drop-othertotpkt
SGW Statistics / S5S8 Total Data Statistics / Downlink	Dropped Pkts Non-Std QCI	s5s8-downlnk-drop-othertotpkt
SGW Statistics / S8 Total Data Statistics / Downlink	Dropped Pkts Non-Std QCI	s8-downlnk-drop-othertotpkt
SGW Statistics / Source Violation	Packets Dropped	srcviolatestat-packets-dropped
	Bytes Dropped	srcviolatestat-bytes-dropped

Web Element Manager Path

- Accounting | Bulk Statistics Configuration | Schema Tab
- Accounting | View/Graph Bulk Statistics | Select Counters and Filters Parameters Tab

PGW Schema Bulk Statistic Enhancements

The following bulk statistics have been added to the PGW schema in WEM Release 12.2.

Table 4-16 PGW Bulk Statistic Enhancements in WEM Release 12.2

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
PGW Schema / Subscriber Session Statistics / Total Bearers Active / Default Bearers	Emergency	sessstat-bearact-emergency-def
	Authentic IMSI	sessstat-bearact-emergency-auth-imsi-def
	Un-Authentic IMSI	sessstat-bearact-emergency-unauth-imsi-def
	Only IMEI	sessstat-bearact-emergency-only-imei-def
PGW Schema / Subscriber Session Statistics / Total Bearers Active / Dedicated Bearers	Emergency	sessstat-bearact-emergency-ded
	Authentic IMSI	sessstat-bearact-emergency-auth-imsi-ded
	Un-Authentic IMSI	sessstat-bearact-emergency-unauth-imsi-ded
	Only IMEI	sessstat-bearact-emergency-only-imei-ded
PGW Schema / Subscriber Session Statistics / Total Bearers Setup / Default Bearers	Emergency	sessstat-bearsetup-emergency-def
	Authentic IMSI	sessstat-bearsetup-emergency-auth-imsi-def
	Only IMEI	sessstat-bearsetup-emergency-only-imei-def
	Un-Authentic IMSI	sessstat-bearsetup-emergency-unauth-imsi-def
PGW Schema / Subscriber Session Statistics / Total Bearers Setup / Dedicated Bearers	UE-Initiated	sessstat-bearsetup-ue-init-ded
	Network-Initiated	sessstat-bearsetup-nw-init-ded
	Emergency	sessstat-bearsetup-emergency-ded
	Authentic IMSI	sessstat-bearsetup-emergency-auth-imsi-ded
	Only IMEI	sessstat-bearsetup-emergency-only-imei-ded
	Un-Authentic IMSI	sessstat-bearsetup-emergency-unauth-imsi-ded
PGW Schema / Subscriber Session Statistics / Total Bearers Rejected / Default Bearers	Total Emergency Default Bearers Rejected	sessstat-bearrej-emergency-def
PGW Schema / Subscriber Session Statistics / Total Bearers Rejected / Dedicated Bearers	Total Emergency Dedicated Bearers Rejected	sessstat-bearrej-emergency-ded

Web Element Manager Path

- Accounting | Bulk Statistics Configuration | Schema Tab
- Accounting | View/Graph Bulk Statistics | Select Counters and Filters Parameters Tab

EGTPC Schema Bulk Statistics Enhancements

The following bulk statistics were added to the EGTPC schema in WEM Release 12.2.

Table 4-17 EGTPC Bulk Statistic Enhancements in WEM Release 12.2

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
EGTPC Statistics / General	Current Sessions	sess-cur
EGTPC Statistics / Tunnel / Create Session Request	Sent	tun-sent-cresess
	Retransmitted Sent	tun-sent-retranscresess
	Received	tun-recv-cresess
	Retransmitted Received	tun-recv-retranscresess
EGTPC Statistics / Tunnel / Create Session Response	Initial Sent	tun-sent-cresessresp
	Accept Sent	tun-sent-cresessrespaccept
	Denied Sent	tun-sent-cresessrespdenied
	Retransmitted Sent	tun-sent-retranscresessresp
	Initial Received	tun-recv-cresessresp
	Accept Received	tun-recv-cresessrespaccept
	Denied Received	tun-recv-cresesssrespdenied
EGTPC Statistics / Tunnel / Modify Bearer Request	Initial Sent	tun-sent-modbearreq
	Retransmitted Sent	tun-sent-retransmodbearreq
	Initial received	tun-recv-modbearreq
	Retransmitted Received	tun-recv-retransmodbearreq
EGTPC Statistics / Tunnel / Modify Bearer Response	Initial Sent	tun-sent-modbearresp
	Accept Sent	tun-sent-modbearrespaccept
	Denied Sent	tun-sent-modbearrespdenied
	Retransmitted Sent	tun-sent-retransmodbearresp
	Initial Received	tun-recv-modbearresp
	Accept Received	tun-recv-modbearrespaccept
	Denied Received	tun-recv-modbearrespdenied
EGTPC Statistics / Tunnel / Delete Session Request	Initial Sent	tun-sent-delsessreq
	Retransmitted Sent	tun-sent-retransdelsessreq
	Initial Received	tun-recv-delsessreq
	Retransmitted Received	tun-recv-retransdelsessreq
EGTPC Statistics / Tunnel / Delete Session Response	Initial Sent	tun-sent-delsessresp
	Accept Sent	tun-sent-delsessrespaccept
	denied Sent	tun-sent-delsessrespdenied
	Initial Received	tun-recv-delsessresp
	Accept received	tun-recv-delsessrespaccept
	Denied Received	tun-recv-delsessrespdenied
EGTPC Statistics / Tunnel / Downlink Data Notification Request	Initial Sent	tun-sent-dlinknotif
	Retransmitted Sent	tun-sent-retransdlinknotif
	Initial Received	tun-recv-dlinknotif
	Retransmitted Received	tun-recv-retransdlinknotif

Table 4-17 EGTPC Bulk Statistic Enhancements in WEM Release 12.2

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
EGTPC Statistics / Tunnel / Downlink Data Notification Acknowledgement	Received	tun-recv-dlinknotifack
	Accept	tun-recv-dlinknotifackaccept
	Denied	tun-recv-dlinknotifackdenied
EGTPC Statistics / Tunnel / Downlink Data Failure Indication	Sent	tun-sent-dlinkdatafail
	Received	tun-recv-dlinkdatafail
EGTPC Statistics / Tunnel / Release Access Bearers Request	Initial Sent	tun-sent-relaccbearreq
	Retransmitted Sent	tun-sent-retransrelaccbearreq
	Initial Receive	tun-recv-relaccbearreq
	Retransmitted Received	tun-recv-retransrelaccbearreq
EGTPC Statistics / Tunnel / Release Access Bearers Response	Initial Sent	tun-sent-relaccbearresp
	Accept Sent	tun-sent-relaccbearrespaccept
	Denied Sent	tun-sent-relaccbearrespdenied
	Retransmitted Sent	tun-sent-retransrelaccbearresp
	Initial Received	tun-recv-relaccbearresp
	Accept Received	tun-recv-relaccbearrespaccept
	Denied Received	tun-recv-relaccbearrespdenied
EGTPC Statistics / Tunnel / Create Bearer Request	Initial Sent	tun-sent-crebear
	Retransmitted Sent	tun-sent-retranscrebear
	Initial Received	tun-recv-crebear
	Retransmitted Received	tun-recv-retranscrebear
EGTPC Statistics / Tunnel / Create Bearer Response	Initial Sent	tun-sent-crebearresp
	Accept Sent	tun-sent-crebearrespaccept
	Denied Sent	tun-sent-crebearrespdenied
	Retransmitted Sent	tun-sent-retranscrebearresp
	Initial Received	tun-recv-crebearresp
	Accept Received	tun-recv-crebearrespaccept
	Denied Received	tun-recv-crebearrespdenied
EGTPC Statistics / Tunnel / Update Bearer Request	Initial Sent	tun-sent-updbearreq
	Retransmitted Sent	tun-sent-retransupdbearreq
	Initial Received	tun-recv-updbearreq
	Transmitted Received	tun-recv-retransupdbearreq
EGTPC Statistics / Tunnel / Update Bearer Response	Initial Sent	tun-sent-updbearresp
	Accept Sent	tun-sent-updbearrespaccept
	Denied Sent	tun-sent-updbearrespdenied
	Initial Received	tun-recv-updbearresp
	Accept Received	tun-recv-updbearrespaccept
	Denied Received	tun-recv-updbearrespdenied

Table 4-17 EGTPC Bulk Statistic Enhancements in WEM Release 12.2

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
EGTPC Statistics / Tunnel / Delete Bearer Request	Initial Sent	tun-sent-delbearreq
	Retransmitted Sent	tun-sent-retransdelbearreq
	Initial received	tun-recv-delbearreq
	Retransmitted Received	tun-recv-retransdelbearreq
EGTPC Statistics / Tunnel / Delete Bearer Response	Initial Sent	tun-sent-delbearresp
	Accept Sent	tun-sent-delbearrespaccept
	Denied Sent	tun-sent-delbearrespdenied
	Initial Received	tun-recv-delbearresp
	Accept Received	tun-recv-delbearrespaccept
	Denied Received	tun-recv-delbearrespdenied
EGTPC Statistics / Tunnel / Bearer Resource Command	Sent	tun-sent-bearrescmd
	Received	tun-recv-bearrescmd
	Failure Sent	tun-sent-bearrescmd-fail
	Failure Received	tun-recv-bearrescmd-fail
	Retrans TX	tun-sent-retransbearrescmd
	Retrans RX	tun-recv-retransbearrescmd
EGTPC Statistics / Tunnel / Bearer Resource Failure Indication	Retrans TX	tun-sent-retransbearrescmd-fail
	Retrans RX	tun-recv-retransbearrescmd-fail
EGTPC Statistics / Tunnel / Modify Bearer Failure Indication	Retrans TX	tun-sent-retransmodbearfail
	Retrans RX	tun-recv-retransmodbearfail
EGTPC Statistics / Tunnel / Delete Bearer Command	Initial TX	tun-sent-delbearcmd
	Retrans TX	tun-sent-retransdelbearcmd
	Initial RX	tun-recv-delbearcmd
	Receive RX	tun-recv-retransdelbearcmd
EGTPC Statistics / Tunnel / Delete Bearer Failure Indication	Initial TX	tun-sent-delbearfail
	Retrans TX	tun-sent-retransdelbearfail
	Initial RX	tun-recv-delbearfail
	Receive RX	tun-recv-retransdelbearfail
EGTPC Statistics / Tunnel / Update User Plane Request	Received	tun-recv-updupanereq
	Retransmitted	tun-recv-retransupduplanereq
EGTPC Statistics / Tunnel / Update User Plane Response	Initial Sent	tun-sent-updupanaresp
	Accept Sent	tun-sent-updupanerespaccept
	Denied Sent	tun-sent-updupanerespdenied

Table 4-17 EGTPC Bulk Statistic Enhancements in WEM Release 12.2

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
EGTPC Statistics / Tunnel / Modify Bearer Command	Sent	tun-sent-modbearcmd
	Received	tun-recv-modbearcmd
	Failure Indication Sent	tun-sent-modbearfail
	Failure Indication Received	tun-recv-modbearfail
	Retrans TX	tun-sent-retransmodbearcmd
	Retrans RX	tun-recv-retransmodbearcmd
EGTPC Statistics / Tunnel / Deactivate Bearer Command	Sent	tun-sent-deactbear
	Received	tun-recv-deactbear
	Failure Indication Sent	tun-sent-deactbearfail
	Failure Indication Received	tun-recv-deactbearfail
EGTPC Statistics / Tunnel / Create Ind Data Forwarding Tunnel Request	Initial TX	tun-sent-creinddatafwdngreq
	Retrans TX	tun-sent-retranscreinddatafwdngreq
	Initial RX	tun-recv-creinddatafwdngreq
	Retrans RX	tun-recv-retranscreinddatafwdngreq
EGTPC Statistics / Tunnel / Create Ind Data Forwarding Tunnel Response	Initial TX	tun-sent-creinddatafwdngrsp
	Accepted TX	tun-sent-creinddatafwdngrspaccept
	Denied TX	tun-sent-creinddatafwdngrspdenied
	Retrans TX	tun-sent-retranscreinddatafwdngrsp
	Initial RX	tun-recv-creinddatafwdngrsp
	Denied RX	tun-recv-creinddatafwdngrspdenied
EGTPC Statistics / Tunnel / Delete Ind Data Forwarding Tunnel Request	Initial TX	tun-sent-delinddatafwdngreq
	Retrans TX	tun-sent-retransdelinddatafwdngreq
	Initial RX	tun-recv-delinddatafwdngreq
	Retrans RX	tun-recv-retransdelinddatafwdngreq
EGTPC Statistics / Tunnel / Delete Ind Data Forwarding Tunnel Response	Initial TX	tun-sent-delinddatafwdngrsp
	Accepted TX	tun-sent-delinddatafwdngrspaccept
	Denied TX	tun-sent-delinddatafwdngrspdenied
	Initial RX	tun-recv-delinddatafwdngrsp
	Accepted RX	tun-recv-delinddatafwdngrspaccept
	Denied RX	tun-recv-delinddatafwdngrspdenied
EGTPC Statistics / Path / Echo Request	Initial Sent	path-sent-echoreq
	Retransmitted Sent	path-sent-retransechoreq
	Initial Receive	path-recv-echoreq
EGTPC Statistics / Path / Echo Response	Total Sent	path-sent-echoresp
	Total Received	path-recv-echoresp
EGTPC Statistics / Path / Version Not Supported	Total Sent	path-sent-versnotsupp
	Total Received	path-recv-versnotsupp

Table 4-17 EGTPC Bulk Statistic Enhancements in WEM Release 12.2

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
EGTPC Statistics / GTP-U Tunnel	G-PDU Sent	gtpv1tun-sent-gpdu
	G-PDU Received	gtpv1tun-recv-gpdu
	T-PDU Octets Sent	gtpv1tun-txoctet
	T-PDU Octets Received	gtpv1tun-rxoctet
	GTP-U Error Indication Sent	gtpv1tun-sent-gtpuerror
	GTP-U Error Indication Received	gtpv1tun-recv-gtpuerror
	GTP-U End Marker Message Sen	gtpv1tun-sent-endmarker
EGTPC Statistics / GTP-U Path	Echo Request Sent	gtpv1path-sent-echoreq
	Echo Request Received	gtpv1path-recv-echoreq
	Echo Response Sent	gtpv1path-sent-echoresp
	Echo Response Received	gtpv1path-recv-echoresp
	Supported Extension Header Notification Sent	gtpv1path-sent-hdrnotif
	Supported Extension Header Notification Received	gtpv1path-recv-hdrnotif
EGTPC Statistics / PGW S5S8	Packets TX	OutSigPktS5S8PGW
	Packets RX	IncSigPktS5S8PGW
	Bytes TX	OutSigOctS5S8PGW
	Bytes RX	IncSigOctS5S8PGW
EGTPC Statistics / SGW S5S8	Packets TX	OutSigPktS5S8SGW
	Packets RX	IncSigPktS5S8SGW
	Bytes TX	OutSigOctS5S8SGW
	Bytes RX	IncSigOctS5S8SGW
EGTPC Statistics / SGW S11S4	Packets TX	OutSigPktS11S4SGW
	Packets RX	IncSigPktS11S4SGW
	Bytes TX	OutSigOctS11S4SGW
	Bytes RX	IncSigOctS11S4SGW
EGTPC Statistics / MME S11S10	Packets TX	OutSigPktS11S10MME
	Packets RX	IncSigPktS11S10MME
	Bytes TX	OutSigOctS11S10MME
	Bytes RX	IncSigOctS11S10MME
EGTPC Statistics / SGSNS4	Packets TX	OutSigPktS4SGSN
	Packets RX	IncSigPktS4SGSN
	Bytes TX	OutSigOctS4SGSN
	Bytes RX	IncSigOctS4SGSN
EGTPC Statistics / Mobility Management Messages / Configuration Transfer Tunnel	Initial RX	mobility-recv-configxfertun
	Initial TX	mobility-sent-configxfertun
EGTPC Statistics / Mobility Management Messages / RAN Information Relay	Initial RX	mobility-recv-ranInforelay
	Initial TX	mobility-sent-ranInforelay

Table 4-17 EGTPC Bulk Statistic Enhancements in WEM Release 12.2

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
EGTPC Statistics / Mobility Management Messages / Context Request	Initial TX	mobility-sent-ctxreq
	Retrans TX	mobility-sent-retransctxreq
	Initial RX	mobility-recv-ctxreq
	Retrans RX	mobility-recv-retransctxreq
EGTPC Statistics / Mobility Management Messages / Context Response	Initial TX	mobility-sent-ctxrsp
	Retrans TX	mobility-sent-retransctxrsp
	Initial RX	mobility-recv-ctxrsp
	Retrans RX	mobility-recv-retransctxrsp
	Accepted TX	mobility-sent-ctxrspaccept
	Denied TX	mobility-sent-ctxrspdenied
	Accepted RX	mobility-recv-ctxrspaccept
	Denied RX	mobility-recv-ctxrspdenied
EGTPC Statistics / Mobility Management Messages / Context Acknowledge	Initial TX	mobility-sent-ctxack
	Retrans TX	mobility-sent-retransctxack
	Initial RX	mobility-recv-ctxack
	Retrans RX	mobility-recv-retransctxack
	Accepted TX	mobility-sent-ctxackaccept
	Denied TX	mobility-sent-ctxackdenied
	Accepted RX	mobility-recv-ctxackaccept
	Denied RX	mobility-recv-ctxackdenied
EGTPC Statistics / Mobility Management Messages / Identification Request	Initial TX	mobility-sent-idtreq
	Retrans TX	mobility-sent-retransidtreq
	Initial RX	mobility-recv-idtreq
	Retrans RX	mobility-recv-retransidtreq
EGTPC Statistics / Mobility Management Messages / Identification Response	Total TX	mobility-sent-idtrsp
	Retrans TX	mobility-sent-retransidtrsp
	Total RX	mobility-recv-idtrsp
	Retrans RX	mobility-recv-retransidtrsp
	Accepted TX	mobility-sent-idtrspaccept
	Denied TX	mobility-sent-idtrspdenied
	Accepted RX	mobility-recv-idtrspaccept
	Denied RX	mobility-recv-idtrspdenied
EGTPC Statistics / Mobility Management Messages / Forward Relocation Request	Initial TX	mobility-sent-fwdrelreq
	Retrans TX	mobility-sent-retransfwdrelreq
	Initial RX	mobility-recv-fwdrelreq
	Retrans RX	mobility-recv-retransfwdrelreq

Table 4-17 EGTPC Bulk Statistic Enhancements in WEM Release 12.2

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
EGTPC Statistics / Mobility Management Messages / Forward Relocation Response	Initial TX	mobility-sent-fwdrelrsp
	Retrans TX	mobility-recv-retransfwdrelrsp
	Initial RX	mobility-sent-fwdrelrspaccept
	Retrans RX	mobility-sent-retransfwdrelrsp
	Initial RX	mobility-recv-fwdrelrsp
	Accepted	mobility-recv-fwdrelrspaccept
	Denied	mobility-recv-fwdrelrspdenied
	Denied TX	mobility-sent-fwdrelrspdenied
EGTPC Statistics / Mobility Management Messages / Forward Access Context Notification	Initial TX	mobility-sent-fwdaccnotif
	Retrans TX	mobility-sent-retransfwdaccnotf
	Initial RX	mobility-recv-fwdaccnotf
	Retrans RX	mobility-recv-retransfwdaccnotf
EGTPC Statistics / Mobility Management Messages / Forward Access Context Acknowledge	Initial TX	mobility-sent-fwdaccack
	Retrans TX	mobility-sent-retransfwdaccack
	Initial RX	mobility-recv-fwdaccack
	Retrans RX	mobility-recv-retransfwdaccack
	Accepted TX	mobility-sent-fwdaccackaccept
	Denied TX	mobility-sent-fwdaccackdenied
	Accepted RX	mobility-recv-fwdaccackaccept
	Denied RX	mobility-recv-fwdaccackdenied
EGTPC Statistics / Mobility Management Messages / Forward Relocation Complete Notification	Initial TX	mobility-sent-fwdrelcmpnotf
	Retrans TX	mobility-sent-retransfwdrelcmpnotf
	Initial RX	mobility-recv-fwdrelcmpnotf
	Retrans RX	mobility-recv-retransfwdrelcmpnotf
EGTPC Statistics / Mobility Management Messages / Forward Relocation Complete Acknowledge	Initial TX	mobility-sent-fwdrelcmpack
	Retrans TX	mobility-sent-retransfwdrelcmpack
	Initial RX	mobility-recv-fwdrelcmpack
	Retrans RX	mobility-recv-retransfwdrelcmpack
	Accepted TX	mobility-sent-fwdrelcmpackaccept
	Denied TX	mobility-sent-fwdrelcmpackdenied
	Accepted RX	mobility-recv-fwdrelcmpackaccept
	Denied RX	mobility-recv-fwdrelcmpackdenied
EGTPC Statistics / Mobility Management Messages / Relocation Cancel Request	Initial TX	mobility-sent-relcancelreq
	Retrans TX	mobility-sent-retransrelcancelreq
	Initial RX	mobility-recv-relcancelreq
	Retrans RX	mobility-recv-retransrelcancelreq

Table 4-17 EGTPC Bulk Statistic Enhancements in WEM Release 12.2

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
EGTPC Statistics / Mobility Management Messages / Relocation Cancel Response	Initial TX	mobility-sent-relcancelrsp
	Retrans TX	mobility-sent-retransrelcancelrsp
	Initial RX	mobility-recv-relcancelrsp
	Retrans RX	mobility-recv-retransrelcancelrsp
	Accepted TX	mobility-sent-relcancelrspaccept
	Denied TX	mobility-sent-relcancelrspdenied
	Accepted RX	mobility-recv-relcancelrspaccept
	Denied RX	mobility-recv-relcancelrspdenied
EGTPC Statistics / Trace Management Messages / Trace Session Activation	Initial Tx	trace-sent-activate
	Initial RX	trace-recv-activate
EGTPC Statistics / Trace Management Messages / Trace Session Deactivation	Initial TX	trace-sent-deactivate
	Initial RX	trace-recv-deactivate
EGTPC Statistics / CS Fallback Messages / Suspend Notification	Initial TX	csfb-sent-suspendnotf
	Retrans TX	csfb-sent-retranssuspendnotf
	Initial RX	csfb-recv-suspendnotf
	Retrans RX	csfb-recv-retranssuspendnotf
EGTPC Statistics / CS Fallback Messages / Suspend Acknowledge	Initial TX	csfb-sent-suspendack
	Accept TX	csfb-sent-suspendackaccept
	Denied TX	csfb-sent-suspendackdenied
	Initial RX	csfb-recv-suspendack
	Accept RX	csfb-recv-suspendackaccept
	Denied RX	csfb-recv-suspenddenied
EGTPC Statistics / CS Fallback Messages / Resume Notification	Initial TX	csfb-sent-resumenotf
	Retrans TX	csfb-sent-retransresumenotf
	Initial RX	csfb-recv-resumenotf
	Retrans RX	csfb-recv-retransresumenotf
EGTPC Statistics / CS Fallback Messages / Resume Acknowledge	Initial TX	csfb-sent-resumeack
	Accept TX	csfb-sent-resumeackaccept
	Denied TX	csfb-sent-resumeackdenied
	Initial RX	csfb-recv-resumeack
	Accept RX	csfb-recv-resumeackaccept
	Denied RX	csfb-recv-resumedenied
EGTPC Statistics / Tunnel Management Messages / Change Notification Request	Initial RX	tun-recv-changenotfreq
	Initial TX	tun-sent-changenotfreq
	Retrans RX	tun-recv-retranschangenotfreq
	Retrans RX	tun-sent-retranschangenotfreq

Table 4-17 EGTPC Bulk Statistic Enhancements in WEM Release 12.2

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
EGTPC Statistics / Tunnel Management Messages / Change Notification Response	Initial RX	tun-recv-changenotfresp
	Accepted RX	tun-recv-changenotfrespaccept
	Denied RX	tun-recv-changenotfrespdenied
	Initial TX	tun-sent-changenotfresp
	Accepted TX	tun-sent-changenotfrespaccept
	Denied TX	tun-sent-changenotfrespdenied
	Retrans TX	tun-sent-retranschangenotfresp

Web Element Manager Path

- Accounting | Bulk Statistics Configuration | Schema Tab
- Accounting | View/Graph Bulk Statistics | Select Counters and Filters Parameters Tab

MME Schema Bulk Statistic Enhancements

The following bulk statistics were added to the MME schema in WEM Release 12.2

Table 4-18 MME Bulk Statistic Schema Enhancements in WEM Release 12.2

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
MME Statistics / S1AP Statistics / Transmitted S1AP Data	MME Config Update	s1ap-transdata-cfgupd
	MME Config Transfer	s1ap-transdata-cfgtfr
MME Statistics / S1AP Statistics / Received S1AP Data	MME Config Update Fail	s1ap-recdata-cfgupdfail
	MME Config Update Ack	s1ap-recdata-cfgupdack
	eNB Config Transfer	s1ap-recdata-enbcfgtfr
MME Statistics / S1AP Statistics / Radio Network Error Statistics	Unknown MME UE S1AP Id	s1ap-err-unknownmme-ues1apid
	Unknown ENB UE S1AP Id	s1ap-err-unknownenb-ues1apid
	Unknown UE S1AP Id Pair	s1ap-err-unknownpair-ues1apid
MME Statistics / S1AP Statistics / Protocol, Error Statistics	Transfer Syntax Error	s1ap-err-tfr-synerr
	Semantic Error	s1ap-err-semanticerr
	Message Not Compatible	s1ap-err-msgnotcompatible
	Abstract Syntax Error - Falsely Constr Msg	s1ap-err-asefalsely-constrmsg
	Abstract Syntax Error - Ignore And Notify	s1ap-err-aseignore-notify
	Abstract Syntax Error - Reject	s1ap-err-aserej
MME Statistics / S1AP Statistics / eNodeB Statistics	Total eNodeB Associations	s1ap-enodeb-assoc
MME Statistics / EMM Statistics / EPS Associations by Attach using IMSI	Attempted	epsattach-imsi-attempted
	Success	epsattach-imsi-success
	Failure	epsattach-imsi-failures

Table 4-18 MME Bulk Statistic Schema Enhancements in WEM Release 12.2

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
MME Statistics / EMM Statistics / EPS Associations by Attach using Local GUTI	Attempted	epsattach-guti-local-attempted
	Success	epsattach-guti-local-success
	Failure	epsattach-guti-local-failures
MME Statistics / EMM Statistics / EPS Associations by Attach using Foreign GUTI	Attempted	epsattach-guti-foreign-attempted
	Success	epsattach-guti-foreign-success
	Failures	epsattach-guti-foreign-failures
MME Statistics / EMM Statistics / EPS Associations by P-TMSI	Attempted	epsattach-ptmsi-attempted
	Success	epsattach-ptmsi-success
	Failures	epsattach-ptmsi-failures
MME Statistics / EMM Statistics / EPS Associations by TAU using Foreign GUTI	Attempted	epstauattach-guti-foreign-attempted
	Success	epstauattach-guti-foreign-success
	Failures	epstauattach-guti-foreign-failures
MME Statistics / EMM Statistics / EPS Associations by TAU using PTMSI	Attempted	epstauattach-ptmsi-attempted
	Success	epstauattach-ptmsi-success
	Failures	epstauattach-ptmsi-failures
MME Statistics / EMM Statistics / EPS Associations for Emergency Bearer Services	Attempted	epsattach-emergency-attempted
	Success	epsattach-emergency-success
	Failure	epsattach-emergency-failures
MME Statistics / EMM Statistics / Associations by Combined Attach using IMSI	Attempted	combinedattach-imsi-attempted
	Success	combinedattach-imsi-success
	Success EPS Only	combinedattach-imsi-success-eps
	Failure	combinedattach-imsi-failure
MME Statistics / EMM Statistics / Associations by Combined Attach using Local GUTI	Attempted	combinedattach-guti-local-attached
	Success	combinedattach-guti-local-success
	Success EPS Only	combinedattach-guti-local-success-eps
	Failure	combinedattach-guti-local-failure
MME Statistics / EMM Statistics / Associations by Combined Attach using Foreign GUTI	Attempted	combinedattach-guti-foreign-attempted
	Success	combinedattach-guti-foreign-success
	Success EPS Only	combinedattach-guti-foreign-success-eps
	Failure	combinedattach-guti-foreign-failure
MME Statistics / EMM Statistics / Associations by Combined Attach using P-TMSI	Attempted	combinedattach-ptmsi-attempted
	Success	combinedattach-ptmsi-success
	Success EPS Only	combinedattach-ptmsi-success-eps
	Failure	combinedattach-ptmsi-failure
MME Statistics / EMM Statistics / Associations by Combined TAU using Foreign GUTI	Attempted	combined-tauattach-guti-foreign-attempted
	Success	combined-tauattach-guti-foreign-success
	Success EPS Only	combined-tauattach-guti-foreign-success-eps
	Failure	combined-tauattach-guti-foreign-failure

Table 4-18 MME Bulk Statistic Schema Enhancements in WEM Release 12.2

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
MME Statistics / EMM Statistics / Associations by Combined TAU using P-TMSI	Attempted	combined-tauattach-ptmsi-attempted
	Success	combined-tauattach-ptmsi-success
	Success EPS Only	combined-tauattach-ptmsi-success-eps
	Failure	combined-tauattach-ptmsi-failure
MME Statistics / EMM Statistics / Periodic TAU	Attempted	tau-periodic-attempted
	Success	tau-periodic-success
	Failures	tau-periodic-failures
MME Statistics / EMM Statistics / Normal TAU without SGW Relocation	Attempted	tau-normal-attempted
	Success	tau-normal-success
	Failures	tau-normal-failures
MME Statistics / EMM Statistics / TAU with Bearer Activation	Attempted	tau-active-attempted
	Success	tau-active-success
	Failures	tau-active-failures
MME Statistics / EMM Statistics / TAU with SGW Relocation	Attempted	tau-sgw-change-attempted
	Success	tau-sgw-change-success
	Failures	tau-sgw-change-failures
MME Statistics / ECM Statistics / Paging Initiation Events	Attempted	paging-init-events-attempted
	Success	paging-init-events-success
	Failures	paging-init-events-failures
	Success At Last eNB	paging-last-enb-success
	Success At Last TAI	paging-last-tai-success
	Success At TAI List	ecmevent-tailist-success
	S1 Release for Load Rebalancing	ecmevent-s1rel-loadbalance
MME Statistics / Total EMM Control Messages / Sent	Attach Accept	emm-msgtx-attach-accept
	Retransmissions	emm-msgtx-attach-accept-retx
	Attach Reject	emm-msgtx-attach-reject
	IMSI Unknown in HSS	emm-msgtx-imsi-unknown-hss
	Illegal UE	emm-msgtx-illegal-ue
	Illegal ME	emm-msgtx-illegal-me
	EPS Not Allowed	emm-msgtx-eps-not-allowed
	Network Failure	emm-msgtx-network-failure
	ESM Failure	emm-msgtx-esm-failure
	Decode Failure	emm-msgtx-decode-failure
	Authentication Reject	emm-msgtx-auth-reject
	Authentication Request	emm-msgtx-auth-req
	Retransmissions	emm-msgtx-auth-req-retx
	Detach Request	emm-msgtx-detach-request

Table 4-18 MME Bulk Statistic Schema Enhancements in WEM Release 12.2

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
MME Statistics / Total EMM Control Messages / Sent (con't)	Retransmissions	emm-msgtx-detach-req-retx
	Reattach Required	emm-msgtx-reattach-req
	Reattach Not Required	emm-msgtx-rettach-not-req
	Detach Accept	emm-msgtx-detach-accept
	Downlink NAS Transport	emm-msgtx-downlink-transport
	EMM Information	emm-msgtx-emm-info
	EMM Status	emm-msgtx-emm-status
	GUTI Relocations	emm-msgtx-guti-reloc
	Retransmissions	emm-msgtx-guti-reloc-retx
	Identity Request	emm-msgtx-identity-req
	Retransmissions	emm-msgtx-identity-req-retx
	Security Mode Command	emm-msgtx-sm-cmd
	Retransmissions	emm-msgtx-sm-cmd-retx
	Service Reject	emm-msgtx-service-reject
	UE Identity Unknown	emm-msgtx-ue-identity-unk
	Implicitly Detached	emm-msgtx-impl-detached
	TAU Accept	emm-msgtx-tau-accept
	Retransmissions	emm-msgtx-tau-accept-retx
	TAU Reject	emm-msgtx-tau-reject
	IMSI Unknown in HSS	emm-msgtx-tau-imsi-unknown-hss
	TAU Illegal UE	emm-msgtx-tau-illegal-ue
	TAU Illegal ME	emm-msgtx-tau-illegal-me
	EPS Not Allowed	emm-msgtx-tau-eps-not-allowed
	TAU Network Fail	emm-msgtx-tau-network-fail
	Decode Failure	emm-msgtx-tau-decode-failure
	No Bearer Active	emm-msgtx-tau-no-bearer-active
	UE Identity Unknown	emm-msgtx-tau-ue-identity-unk
	Implicit Detached	emm-msgtx-tau-implicit-detached
	IMEI Not Accepted	emm-msgtx-imei-not-accept
	No suitable cells in TA	emm-msgtx-no-suitable-cell-ta
	PLMN Not Allowed	emm-msgtx-plmn-not-allow
	Roaming Restricted TA	emm-msgtx-roaming-restrict-ta
	TA Not Allowed	emm-msgtx-ta-not-allow
	TAU - CS Service Notification	emm-msgtx-tau-cs-service-notif
	TAU - IMEI not accepted	emm-msgtx-tau-imei-not-accept
	TAU - No suitable cells in TA	emm-msgtx-tau-no-suitable-cell-ta
	TAU - PLMN not allowed	emm-msgtx-tau-plmn-not-allow
	TAU - Roaming Restricted TA	emm-msgtx-tau-roaming-restrict-ta
	TAU - TA not allowed	emm-msgtx-tau-ta-not-allow

Table 4-18 MME Bulk Statistic Schema Enhancements in WEM Release 12.2

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
MME Statistics / Total EMM Control Messages / Received	Clear Text Messages	emm-msgrx-plain-nas
	Integrity-check Enabled	emm-msgrx-integrity
	Ciphered Messages	emm-msgrx-ciphered
	Accepted	emm-msgrx-accepted
	Ignored Messages	emm-msgrx-discarded
	Decode Failures	emm-msgrx-decode-failure
	Attach Complete	emm-msgrx-attach-complete
	Denied	emm-msgrx-denied
	Attach Request	emm-msgrx-attach-req
	Retransmissions	emm-msgrx-attach-retx
	Authentication Failure	emm-msgrx-auth-failure
	Authentication Response	emm-msgrx-auth-resp
	Switch Off	emm-msgrx-detach-req-switchoff
	Not Switchoff	emm-msgrx-detach-req-not-switchoff
	Detach Request	emm-msgrx-detach-req
	IMSI Detach	emm-msgrx-imsi-detach
	EMM Status	emm-msgrx-emm-status
	GUTI Reloc Complete	emm-msgrx-guti-reloc-complete
	Security Mode Complete	emm-msgrx-sm-complete
	Security Mode Reject	emm-msgrx-sm-reject
	Service Request	emm-msgrx-service-req
	TAU Request	emm-msgrx-tau-req
	Retransmissions	emm-msgrx-tau-retx
	TAU Complete	emm-msgrx-tau-complete
	Extended Service Request	emm-msgrx-ext-service-req
	Identity Response	emm-msgrx-identity-resp
MME Statistics / Total ESM Control Messages / Received	Clear-text messages	esm-msgrx-plain-nas
	Accepted	esm-msgrx-accepted
	Brr Rsrc Alloc Request	esm-msgrx-brr-rsrc-alloc-req
	Brr Rsrc Modify Request	esm-msgrx-brr-rsrc-modify-req
	Ciphered messages	esm-msgrx-ciphered
	Act Dedicated Brr Accept	esm-msgrx-ded-brr-accept
	Act Dedicated Brr Reject	esm-msgrx-ded-brr-reject
	Denied	esm-msgrx-denied
	Act Default Brr Accept	esm-msgrx-dflt-brr-accept
	Act Default Brr Reject	esm-msgrx-dflt-brr-reject
	ESM Status	esm-msgrx-em-status
	ESM Information Response	esm-msgrx-esm-info-resp

Table 4-18 MME Bulk Statistic Schema Enhancements in WEM Release 12.2

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
MME Statistics / Total ESM Control Messages / Received (con't)	Integrity-check enabled	esm-msgrx-integrity
	Modify Brr Ctxt Accept	esm-msgrx-mod-brr-accept
	Modify Brr Ctxt Reject	esm-msgrx-mod-brr-reject
	PDN Connectivity Request	esm-msgrx-pdn-con-req
	PDN Disconnect Request	esm-msgrx-pdn-discon-req
	Deactivate Brr Accept	esm-msgrx-deactivate-brr-accept
MME Statistics / Total ESM Control Messages / Sent	Act Dedicated Bearer	esm-msgtx-act-ded-brr
	Retransmissions	esm-msgtx-act-ded-brr-retx
	Act Default Bearer	esm-msgtx-act-dflt-brr
	Retransmissions	esm-msgtx-act-dflt_bee-retx
	Bearer Alloc Reject	esm-msgtx-brralloc-rej
	Collision with NW Op	esm-msgtx-brralloc-rej-collision-nwop
	Invalid Bearer Id	esm-msgtx-brralloc-rej-invalid-brrid
	Invalid PTI	esm-msgtx-brralloc-rej-invalid-pti
	PTI Already in Use	esm-msgtx-brralloc-rej-pt1-inuse
	Semantic Error TFT	esm-msgtx-brralloc-rej-semantic-errtft
	Syntactic Error TFT	esm-msgtx-brralloc-rej-syntactic-errtft
	Bearer Modify Reject	esm-msgtx-brrmod-rej
	PTI Already in Use	esm-msgtx-brrmod-rej-pti-inuse
	Semantic Error TFT	esm-msgtx-brrmod-rej-semantic-errtft
	Syntactic Error TFT	esm-msgtx-brrmod-rej-syntactic-errtft
	Invalid Bearer ID	esm-msgtx-brrmod-rej-invalid-brrid
	Collision with NW Op	esm-msgtx-brrmod-rej-collision-nwop
	Rejected By PGW/SGW	esm-msgtx-brrmod-rej-pgw-rej
	Invalid PTI	esm-msgtx-brrmod-rej-invalid-pti
	Deactivate Bearer	esm-msgtx-deactbrr
	Retransmissions	esm-msgtx-deactbrr-retx
	ESM Information Req	esm-msgtx-deactbrr-esm-info-req
	Retransmissions	esm-msgtx-deactbrr-esm-info-req-retx
	Modify Bearer	esm-msgtx-deactbrr-modbrr
	Retransmissions	esm-msgtx-deactbrr-moderr-retx
	PDN Connectivity Reject	esm-msgtx-pdncon-rej
	PTI Already in Use	esm-msgtx-pdncon-rej-pti-inuse
	Unknown or Missing APN	esm-msgtx-pdncon-rej-apn-unk
	Unknown PDN Type	esm-msgtx-pdncon-rej-pdntype-unk
	Invalid Bearer ID	esm-msgtx-pdncon-rej-inv-brrid
	Invalid PTI	esm-msgtx-pdncon-rej-inv-pti
	Rejected By PGW/SGW	esm-msgtx-pdncon-rej-pgw-rej

Table 4-18 MME Bulk Statistic Schema Enhancements in WEM Release 12.2

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
MME Statistics / Total ESM Control Messages / Sent (con't)	PDN Disconnect Reject	esm-msgtx-pdndiscon-rej
	PTI Already in Use	esm-msgtx-pdndiscon-rej-pti-inuse
	Last PDN Disconnection	esm-msgtx-pdndiscon-rej-lastpdn
	Invalid PTI	esm-msgtx-pdndiscon-rej-inv-pti
	Invalid Bearer ID	esm-msgtx-pdndiscon-rej-inv-brrid
	Rejected By PGW/SGW	esm-msgtx-pdndiscon-rej-pgw-rej
	Bearer Alloc Reject - Insufficient Resources	esm-msgtx-brralloc-rej-insuff-resource
	Bearer Modify Reject - Insufficient Resources	esm-msgtx-brrmod-rej-insuff-resource
MME Statistics / ESM Statistics / UE Initiated PDN Disconnections	Attempted	pdn-disconnect-ue-attempted
	Success	pdn-disconnect-ue-success
	Failure	pdn-disconnect-ue-failures
MME Statistics / ESM Statistics / MME Initiated PDN Disconnections	Attempted	pdn-disconnect-mme-attempted
	Success	pdn-disconnect-mme-success
	Failure	pdn-disconnect-mme-failures
MME Statistics / ESM Statistics / PGW/SGW Initiated PDN Disconnections	Attempted	pdn-disconnect-pgw-attempted
	Success	pdn-disconnect-pgw-success
	Failure	pdn-disconnect-pgw-failures
MME Statistics / ESM Statistics / HSS Initiated PDN Disconnections	Attempted	pdn-disconnect-hss-attempted
	Success	pdn-disconnect-hss-success
	Failure	pdn-disconnect-hss-failures
MME Statistics / ESM Statistics / UE Initiated Dedicated Bearer Activations	Attempted	dedi-brr-activation-ue-attempted
	Success	dedi-brr-activation-ue-success
	Failure	dedi-brr-activation-ue-failures
MME Statistics / ESM Statistics / MME Initiated Bearer Deactivations	Attempted	brr-deactivation-mme-attempted
	Success	brr-deactivation-mme-success
	Failure	brr-deactivation-mme-failures
MME Statistics / ESM Statistics / PGW / SGW Initiated Bearer Deactivations	Attempted	brr-deactivation-pgw-attempted
	Success	brr-deactivation-pgw-success
	Failure	brr-deactivation-pgw-failures
MME Statistics / ESM Statistics / UE Initiated Bearer Deactivations	Attempted	brr-deactivation-ue-attempted
	Success	brr-deactivation-ue-success
	Failure	brr-deactivation-ue-failures
MME Statistics / ESM Statistics / HSS Initiated Bearer Modifications	Attempted	brr-modification-hss-attempted
	Success	brr-modification-hss-success
	Failure	brr-modification-hss-failures

Table 4-18 MME Bulk Statistic Schema Enhancements in WEM Release 12.2

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
MME Statistics / ESM Statistics / PGW/SGW Initiated Bearer Modifications	Attempted	brr-modification-pgw-attemted
	Success	brr-modification-pgw-success
	Failure	brr-modification-pgw-failures
MME Statistics / ESM Statistics / UE Initiated Bearer Modifications	Attempted	brr-modification-ue-attempted
	Success	brr-modification-ue-success
	Failure	brr-modification-ue-failures
MME Statistics / EUTRAN - EUTRAN using S10 Interface / Outbound relocation using TAU Procedure	Attempted	out-tau-ho-4gto4g-s10-attempted
	Success	out-tau-ho-4gto4g-s10-success
	Failures	out-tau-ho-4gto4g-s10-failures
MME Statistics / EUTRAN - EUTRAN using S10 Interface / Outbound relocation using S1 HO Procedure	Attempted	out-s1-ho-4gto4g-s10-attempted
	Success	out-s1-ho-4gto4g-s10-success
	Failures	out-s1-ho-4gto4g-s10-failures
MME Statistics / EUTRAN - EUTRAN using S10 Interface / Inbound relocation using TAU Procedure	Attempted	in-tau-ho-4gto4g-s10-attempted
	Success	in-tau-ho-4gto4g-s10-success
	Failures	in-tau-ho-4gto4g-s10-failures
MME Statistics / EUTRAN - EUTRAN using S10 Interface / Inbound relocation using S1 HO Procedure	Attempted	in-s1-ho-4gto4g-s10-attempted
	Success	in-s1-ho-4gto4g-s10-success
	Failures	in-s1-ho-4gto4g-s10-failures
MME Statistics / EUTRAN - UTRAN using GnGp Interface / Outbound Relocation using S1 HO Procedure	Attempted	out-s1-ho-4gto3g-gngp-attempted
	Success	out-s1-ho-4gto3g-gngp-success
	Failures	out-s1-ho-4gto3g-gngp-failures
MME Statistics / EUTRAN - UTRAN using GnGp Interface / Inbound Relocation using S1 HO Procedure	Attempted	in-s1-ho-3gto4g-gngp-attempted
	Success	in-s1-ho-3gto4g-gngp-success
	Failures	in-s1-ho-3gto4g-gngp-failures
MME Statistics / EUTRAN - GERAN using GnGp Interface / Outbound relocation using S1 HO Procedure	Attempted	out-s1-ho-4gto2g-gngp-attempted
	Success	out-s1-ho-4gto2g-gngp-success
	Failures	out-s1-ho-4gto2g-gngp-failures
MME Statistics / EUTRAN - GERAN using GnGp Interface / Inbound relocation using S1 HO Procedure	Attempted	in-s1-ho-2gto4g-gngp-attempted
	Success	in-s1-ho-2gto4g-gngp-success
	Failures	in-s1-ho-2gto4g-gngp-failures
MME Statistics / EUTRAN - GERAN A/Gb Mode Inter-RAT Handovers using S3 Interface / Inbound Relocation	Attempted	in-s1-ho-2gto4g-s3-attempted
	Success	in-s1-ho-2gto4g-s3-success
	Failures	in-s1-ho-2gto4g-s3-failures
MME Statistics / EUTRAN - GERAN A/Gb Mode Inter-RAT Handovers using S3 Interface / Outbound Relocation	Attempted	out-s1-ho-4gto3g-s3-attempted
	Success	out-s1-ho-4gto3g-s3-success
	Failures	out-s1-ho-4gto3g-s3-failures

Table 4-18 MME Bulk Statistic Schema Enhancements in WEM Release 12.2

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
MME Statistics / EUTRAN - UTRAN Iu mode Inter-RAT Handovers using S3 Interface / Inbound Relocation	Attempted	in-s1-ho-3gto4g-s3-attempted
	Success	in-s1-ho-3gto4g-s3-success
	Failures	in-s1-ho-3gto4g-s3-failures
MME Statistics / EUTRAN - UTRAN Iu mode Inter-RAT Handovers using S3 Interface / Outbound Relocation	Attempted	out-s1-ho-4gto2g-s3-attempted
	Success	out-s1-ho-4gto2g-s3-success
	Failures	out-s1-ho-4gto2g-s3-failures
MME Statistics / EUTRAN - UTRAN/GERAN Iu or A/Gb mode Cell Reselections using Gn/Gp Interface / Inbound Relocation using TAU Procedure	Attempted	out-rau-ho-4gto3g2g-gngp-attempted
	Success	out-rau-ho-4gto3g2g-gngp-success
	Failures	out-rau-ho-4gto3g2g-gngp-failures
MME Statistics / EUTRAN - UTRAN/GERAN Iu or A/Gb mode Cell Reselections using Gn/Gp Interface / Outbound Relocation using RAU Procedure	Attempted	in-tau-ho-2g3gto4g-gngp-attempted
	Success	in-tau-ho-2g3gto4g-gngp-success
	Failures	in-tau-ho-2g3gto4g-gngp-failures
MME Statistics / EUTRAN - UTRAN/GERAN Iu or A/Gb mode Cell Reselections using S3 Interface / Outbound Relocation using RAU Procedure	Attempted	in-tau-ho-2g3gto4g-s3-attempted
	Success	in-tau-ho-2g3gto4g-s3-success
	Failures	in-tau-ho-2g3gto4g-s3-failures
MME Statistics / EUTRAN - UTRAN/GERAN Iu or A/Gb mode Cell Reselections using S3 Interface / Inbound Relocation using TAU Procedure	Attempted	out-rau-ho-4gto3g2g-s3-attempted
	Success	out-rau-ho-4gto3g2g-s3-success
	Failures	out-rau-ho-4gto3g2g-s3-failures
MME Statistics / EUTRAN - UTRAN/GERAN using Sv Interface / CS only Handover with no DTM Support	Attempted	s1-ho-4gto3g-cs-nodtm-sv-attempted
	Success	s1-ho-4gto3g-cs-nodtm-sv-success
	Failures	s1-ho-4gto3g-cs-nodtm-sv-failures
MME Statistics / EUTRAN - UTRAN/GERAN using Sv Interface / CS Only Handover	Attempted	s1-ho-4gto3g-cs-sv-attempted
	Success	s1-ho-4gto3g-cs-sv-success
	Failures	s1-ho-4gto3g-cs-sv-failures
MME Statistics / EUTRAN - UTRAN/GERAN using Sv Interface / CS and PS Handover	Attempted	s1-ho-4gto3g-csps-sv-attempted
	Success	s1-ho-4gto3g-csps-sv-success
	Failures	s1-ho-4gto3g-csps-sv-failures
MME Statistics / EUTRAN - UTRAN/GERAN using Sv Interface / PDN Statistics	All PDNs	pdn-all
	Connected PDNs	pdn-connected
	Idle PDNs	pdn-idle
MME Statistics / EUTRAN - UTRAN/GERAN using Sv Interface / Emergency PDN Statistics	All PDNs	pdn-emergency-all
	Connected PDNs	pdn-emergency-connected
	Idle PDNs	pdn-emergency-idle

Table 4-18 MME Bulk Statistic Schema Enhancements in WEM Release 12.2

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
MME Statistics / EUTRAN - UTRAN/GERAN using Sv Interface / Bearer Statistics	All Bearers	brr-all
	Connected Bearers	brr-connected
	Idle Bearers	brr-idle
MME Statistics / EUTRAN - UTRAN/GERAN using Sv Interface / Session Statistics	Attached Calls	sess-call-all
	Connected Calls	sess-call-connected
	Idle Calls	sess-call-idle
	Emergency Session Statistics - Attached Calls	sess-emergency-call-all
	Emergency Session Statistics - Connected Calls	sess-emergency-call-connected
	Emergency Session Statistics - Connected Calls	sess-emergency-call-idle
	Emergency Session Statistics - Idle Calls	sess-emergency-call-idle
	Unauthenticated Session Statistics - Attached Calls	sess-unauth-call-all
	Unauthenticated Session Statistics - Connected Calls	sess-unauth-call-idle
	Total Connected Sessions	sess-ecm-connect

MAP Schema Bulk Statistic Enhancements

The following bulk statistics have been added to the MAP schema in WEM Release 12.2.

Table 4-19 MAP Bulk Statistic Enhancements in WEM Release 12.2

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
MAP Schema / Map Statistics	Open Request TX	map-open-req-tx
	Open Request RX	map-open-req-rx
	Open Response TX	map-open-rsp-tx
	Open Response RX	map-open-rsp-rx
	Close Request TX	map-close-tx
	Close Request RX	map-close-rx
	Abort Request TX	map-abort-tx
	Abort Request RX	map-abort-rx
	HLR RESET RX	map-hlr-reset-rcvd
MAP Schema / Map Statistics / Authentication	Request TX	map-auth-req-tx
	Successful	map-auth-succes
	Failed	map-auth-fail
	Timed Out	map-auth-timeouts-rcvd

Table 4-19 MAP Bulk Statistic Enhancements in WEM Release 12.2

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
MAP Schema / Map Statistics / Check IMEI	Request TX	map-imei-req-tx
	Successful	map-imei-succes
	Failed	map-imei-fail
	Timed Out	map-imei-timeout
MAP Schema / Map Statistics / GPRS Location Update	Request TX	map-gprs-update-loc-req-tx
	Successful	map-gprs-update-loc-rsp-tx
	Failed	map-gprs-update-loc-err-tx
	Timed Out	map-gprs-update-loc-timeouts-rx
MAP Schema / Map Statistics / Subscriber Location	Request TX	map-sub-loc-rpt-req-tx
	Successful	map-sub-loc-rpt-rsp-tx
	Failed	map-sub-loc-rpt-err-tx
	Timed Out	map-sub-loc-rpt-timeouts-rx
MAP Schema / Map Statistics / Provide Subscriber Location	Request RX	map-prov-sub-loc-req-rx
	Successful Response TX	map-prov-sub-loc-rsp-tx
	Failure Response TX	map-prov-sub-loc-err-tx
MAP Schema / Map Statistics / Cancel Location	Request RX	map-cancel-loc-req-rx
	Successful Response TX	map-cancel-loc-rsp-tx
	Failure Response TX	map-cancel-loc-err-tx
MAP Schema / Map Statistics / Delete Subscriber Data	Request RX	map-del-subs-req-rx
	Successful Response TX	map-del-subs-rsp-tx
	Failure Response TX	map-del-subs-ret-tx
MAP Schema / Map Statistics / Insert Subscriber	Data(ISD)Requests RX	map-insert-subs-rcvd
	StandAlone ISD Request RX	map-standalone-isd-rcvd
	ISD Response TX	map-isd-rsp-tx
	ISD Failure Response TX	map-isd-err-tx
MAP Schema / Map Statistics / Authentication Failure Report	Request TX	map-auth-fail-rept-req-tx
	Successful	map-auth-fail-rept-rsp-rx
	Failed	map-auth-fail-rept-err-rx
	Timed Out	map-auth-fail-rept-timeouts-rcvd
MAP Schema / Map Statistics / Purge	Request TX	map-purge-req-tx
	Successful	map-purge-success
	Failed	map-purge-fail
	Timed Out	map-purge-timeouts-rcvd
MAP Schema / Map Statistics / MO Forward	Request TX	map-mo-fwd-req-sent
	Successful	map-mo-fwd-rsp-rcvd
	Failed	map-mo-fwd-rsp-failed
	Timed Out	map-mo-fwd-rsp-time-out

Table 4-19 MAP Bulk Statistic Enhancements in WEM Release 12.2

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
MAP Schema / Map Statistics / MT Forward	Request RX	map-mt-fwd-req-sent
	Successful Response Tx	map-mt-fwd-rsp-rcvd
	Failure Response Tx	map-mt-fwd-rsp-failed
MAP Schema / Map Statistics / Ready for SM	Request TX	map-ready-for-sm-req
	Successful	map-ready-for-sm-rsp
	Failure	map-ready-for-sm-rsp-failed
	Timed Out	map-ready-for-sm-rsp-time-out

Web Element Manager Path

- Accounting | Bulk Statistics Configuration | Schema Tab
- Accounting | View/Graph Bulk Statistics | Select Counters and Filters Parameters Tab

ASNGW Schema Bulk Statistic Enhancements

The following bulk statistics have been added to the ASNGW schema in WEM Release 12.2.

Table 4-20 ASNGW Bulk Statistic Enhancements in WEM Release 12.2

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
ASNGW / R6 Messages / R6 Keep Alive Request Message	Total Sent	r6keepalivereq-totsent
	Retransmissions Sent	r6keepalivereq-retranssent
	Total Send Failures	r6keepalivereq-totsendfail
	Total Received	r6keepalivereq-totrec
	Total Accepted	r6keepalivereq-totacc
	Total Relayed	r6keepalivereq-totrelay
	Total Denied	r6keepalivereq-totdenied
	Total Discarded	r6keepalivereq-totdiscard
	Badly Formed	r6keepalivereq-badform
	Decode Error	r6keepalivereq-decodeerr
	Unspecified Error	r6keepalivereq-unspecerr
	TLV Value Invalid	r6keepalivereq-tlvvalinval
	Missing Mandatory TLV	r6keepalivereq-missmandtlv
	Unknown TLV	r6keepalivereq-unknowntlv
	Duplicate TLV Found	r6keepalivereq-duptlvfound
	No Session Found	r6keepalivereq-nosessfound
	No Resource Drops	r6keepalivereq-noresourcedrop
	Admin Prohibited	r6keepalivereq-admprohibit
	Transaction ID Error	r6keepalivereq-transiderr
ASNGW / R6 Messages / R6 Keep Alive Response Message	Total Sent	r6keepaliversp-totsent
	Retransmissions Sent	r6keepaliversp-retranssent

Table 4-20 ASNGW Bulk Statistic Enhancements in WEM Release 12.2

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
	Total Send Failures	r6keepaliversp-totsendfail
	Total Received	r6keepaliversp-totrec
	Total Accepted	r6keepaliversp-totacc
	Total Relayed	r6keepaliversp-totrelay
	Total Denied	r6keepaliversp-totdenied
	Total Discarded	r6keepaliversp-totdiscard
	Badly Formed	r6keepaliversp-badform
	Decode Error	r6keepaliversp-decodeerr
	Unspecified Error	r6keepaliversp-unspecerr
	TLV Value Invalid	r6keepaliversp-tlvvalinval
	Missing Mandatory TLV	r6keepaliversp-missmandtlv
	Unknown TLV	r6keepaliversp-unknowntlv
	Duplicate TLV Found	r6keepaliversp-duptlvfound
	No Session Found	r6keepaliversp-nosessfound
	No Resource Drops	r6keepaliversp-noresourcedrop
	Admin Prohibited	r6keepaliversp-admprohibit
	Transaction ID Error	r6keepaliversp-transiderr

Web Element Manager Path

- Accounting | Bulk Statistics Configuration | Schema Tab
- Accounting | View/Graph Bulk Statistics | Select Counters and Filters Parameters Tab

RP Schema Bulk Statistic Enhancements

The following bulk statistics have been added to the RP schema in WEM Release 12.2.

Table 4-21 RP Schema Bulk Statistic Enhancements in WEM Release 12.2

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
RP / Session Update Send Reason	Always On Indication	sess-always-on-indication

Web Element Manager Path

- Accounting | Bulk Statistics Configuration | Schema Tab
- Accounting | View/Graph Bulk Statistics | Select Counters and Filters Parameters Tab

ASNPC Schema Bulk Statistic Enhancements

The following bulk statistics have been added to the ASNPC schema in WEM Release 12.2.

Table 4-22 ASNPC Schema Bulk Statistic Enhancements in WEM Release 12.2

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
ASNPC Statistics / R6 Messages / R6 Idle Mode Entry MS State Change Request Msg	Total Sent	r6imentstachareq-totsent
	Retransmissions Sent	r6imentstachareq-retranssent
	Total Send Failures	r6imentstachareq-totsendfail
	Total Received	r6imentstachareq-totrec
	Total Accepted	r6imentstachareq-totacc
	Total Relayed	r6imentstachareq-totrelay
	Total Denied	r6imentstachareq-totdenied
	Total Discarded	r6imentstachareq-totdiscard
	Badly Formed	r6imentstachareq-badform
	Decode Error	r6imentstachareq-decodeerr
	Unspecified Error	r6imentstachareq-unspecerr
	Missing Mandatory TLV	r6imentstachareq-missmandtlv
	TLV Value Invalid	r6imentstachareq-tlvvalinval
	Unknown TLV	r6imentstachareq-unknowntlv
	Duplicate TLV Found	r6imentstachareq-duptlvfound
	No Session Found	r6imentstachareq-nosessfound
	Admin Prohibited	r6imentstachareq-admprohibit
	No Resource Drops	r6imentstachareq-noresourcedrop
	Trans ID Error	r6imentstachareq-transiderr
ASNPC Statistics / R6 Messages / R6 Idle Mode Entry MS State Change Response Msg	Total Sent	r6imentstacharsp-totsent
	Retransmissions Sent	r6imentstacharsp-retranssent
	Total Send Failures	r6imentstacharsp-totsendfail
	Total Received	r6imentstacharsp-totrec
	Total Accepted	r6imentstacharsp-totacc
	Total Relayed	r6imentstacharsp-totrelay
	Total Denied	r6imentstacharsp-totdenied
	Total Discarded	r6imentstacharsp-totdiscard
	Badly Formed	r6imentstacharsp-badform
	Decode Error	r6imentstacharsp-decodeerr
	Unspecified Error	r6imentstacharsp-unspecerr
	Missing Mandatory TLV	r6imentstacharsp-missmandtlv
	TLV Value Invalid	r6imentstacharsp-tlvvalinval
	Unknown TLV	r6imentstacharsp-unknowntlv
	Duplicate TLV Found	r6imentstacharsp-duptlvfound
	No Session Found	r6imentstacharsp-nosessfound
	Admin Prohibited	r6imentstacharsp-admprohibit
	No Resource Drops	r6imentstacharsp-noresourcedrop
	Trans ID Error	r6imentstacharsp-transiderr

Table 4-22 ASNPC Schema Bulk Statistic Enhancements in WEM Release 12.2

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
ASNPC Statistics / R6 Messages / R6 Idle Mode Entry MS State Change Ack Msg	Total Sent	r6imentstachaack-totsent
	Retransmissions Sent	r6imentstachaack-retranssent
	Total Send Failures	r6imentstachaack-totsendfail
	Total Received	r6imentstachaack-totrec
	Total Accepted	r6imentstachaack-totacc
	Trans ID Error	r6imentstachaack-transiderr
ASNPC Statistics / R6 Messages / R6 Idle Mode Exit MS State Change Request Msg	Total Sent	r6imexitstachareq-totsent
	Retransmissions Sent	r6imexitstachareq-retranssent
	Total Send Failures	r6imexitstachareq-totsendfail
	Total Received	r6imexitstachareq-totrec
	Total Accepted	r6imexitstachareq-totacc
	Total Relayed	r6imexitstachareq-totrelay
	Total Denied	r6imexitstachareq-totdenied
	Total Discarded	r6imexitstachareq-totdiscard
	Badly Formed	r6imexitstachareq-badform
	Decode Error	r6imexitstachareq-decodeerr
	Unspecified Error	r6imexitstachareq-unspecerr
	Missing Mandatory TLV	r6imexitstachareq-missmandtlv
	TLV Value Invalid	r6imexitstachareq-tlvvalinval
	Unknown TLV	r6imexitstachareq-unknowntlv
	Duplicate TLV Found	r6imexitstachareq-duptlvfound
	No Session Found	r6imexitstachareq-nosessfound
	Admin Prohibited	r6imexitstachareq-admprohibit
	No Resource Drops	r6imexitstachareq-noresourcedrop
	Trans ID Error	r6imexitstachareq-transiderr

Table 4-22 ASNPC Schema Bulk Statistic Enhancements in WEM Release 12.2

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
ASNPC Statistics / R6 Messages / R6 Idle Mode Exit MS State Change Response Msg	Total Sent	r6imexitstacharsp-totsent
	Retransmissions Sent	r6imexitstacharsp-retranssent
	Total Send Failures	r6imexitstacharsp-totsendfail
	Total Received	r6imexitstacharsp-totrec
	Total Accepted	r6imexitstacharsp-totacc
	Total Relayed	r6imexitstacharsp-totrelay
	Total Denied	r6imexitstacharsp-totdenied
	Total Discarded	r6imexitstacharsp-totdiscard
	Badly Formed	r6imexitstacharsp-badform
	Decode Error	r6imexitstacharsp-decodeerr
	Unspecified Error	r6imexitstacharsp-unspecerr
	Missing Mandatory TLV	r6imexitstacharsp-missmandtlv
	TLV Value Invalid	r6imexitstacharsp-tlvvalinval
	Unknown TLV	r6imexitstacharsp-unknowntlv
	Duplicate TLV Found	r6imexitstacharsp-duptlvfound
	No Session Found	r6imexitstacharsp-nosessfound
	Admin Prohibited	r6imexitstacharespadmprohibit
	No Resource Drops	r6imexitstacharsp-noresourcedrop
	Trans ID Error	r6imexitstacharsp-transiderr
ASNPC Statistics / R6 Messages / R6 Location Update Request Msg	Total Sent	r6locupdreq-totsent
	Retransmissions Sent	r6locupdreq-retranssent
	Total Send Failures	r6locupdreq-totsendfail
	Total Received	r6locupdreq-totrec
	Total Accepted	r6locupdreq-totacc
	Total Relayed	r6locupdreq-totrelay
	Total Denied	r6locupdreq-totdenied
	Total Discarded	r6locupdreq-totdiscard
	Badly Formed	r6locupdreq-badform
	Decode Error	r6locupdreq-decodeerr
	Unspecified Error	r6locupdreq-unspecerr
	Missing Mandatory TLV	r6locupdreq-missmandtlv
	TLV Value Invalid	r6locupdreq-tlvvalinval
	Unknown TLV	r6locupdreq-unknowntlv
	Duplicate TLV Found	r6locupdreq-duptlvfound
	No Session Found	r6locupdreq-nosessfound
	Admin Prohibited	r6locupdreq-admprohibit
	No Resource Drops	r6locupdreq-noresourcedrop
	Trans ID Error	r6locupdreq-transiderr

Table 4-22 ASNPC Schema Bulk Statistic Enhancements in WEM Release 12.2

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
ASNPC Statistics / R6 Messages / R6 Location Update Response Msg	Total Sent	r6locupdrsp-totsent
	Retransmissions Sent	r6locupdrsp-retranssent
	Total Send Failures	r6locupdrsp-totsendfail
	Total Received	r6locupdrsp-totrec
	Total Accepted	r6locupdrsp-totacc
	Total Relayed	r6locupdrsp-totrelay
	Total Denied	r6locupdrsp-totdenied
	Total Discarded	r6locupdrsp-totdiscard
	Badly Formed	r6locupdrsp-badform
	Decode Error	r6locupdrsp-decodeerr
	Unspecified Error	r6locupdrsp-unspecerr
	Missing Mandatory TLV	r6locupdrsp-missmandtlv
	TLV Value Invalid	r6locupdrsp-tlvvalinval
	Unknown TLV	r6locupdrsp-unknowntlv
	Duplicate TLV Found	r6locupdrsp-duptlvfound
	No Session Found	r6locupdrsp-nosessfound
	Admin Prohibited	r6locupdreq-admprohibit
	No Resource Drops	r6locupdrsp-noresourcedrop
	Trans ID Error	r6locupdrsp-transiderr
ASNPC Statistics / R6 Messages / R6 Location Update Confirm Msg	Total Sent	r6locupdcnf-totsent
	Retransmissions Sent	r6locupdcnf-retranssent
	Total Send Failures	r6locupdcnf-totsendfail
	Total Received	r6locupdcnf-totrec
	Total Accepted	r6locupdcnf-totacc
	Total Relayed	r6locupdcnf-totrelay
	Total Denied	r6locupdcnf-totdenied
	Total Discarded	r6locupdcnf-totdiscard
	Badly Formed	r6locupdcnf-badform
	Decode Error	r6locupdcnf-decodeerr
	Unspecified Error	r6locupdcnf-unspecerr
	Missing Mandatory TLV	r6locupdcnf-missmandtlv
	TLV Value Invalid	r6locupdcnf-tlvvalinval
	Unknown TLV	r6locupdcnf-unknowntlv
	Duplicate TLV Found	r6locupdcnf-duptlvfound
	No Session Found	r6locupdcnf-nosessfound
	Admin Prohibited	r6locupdcnf-admprohibit
	No Resource Drops	r6locupdcnf-noresourcedrop
	Trans ID Error	r6locupdcnf-transiderr

Table 4-22 ASNPC Schema Bulk Statistic Enhancements in WEM Release 12.2

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
ASNPC Statistics / R6 Messages / R6 Paging Announce Msg	Total Sent	r6pagannouce-totsent
	Retransmissions Sent	r6pagannouce-retranssent
	Total Send Failures	r6pagannouce-totsendfail
	Total Received	r6pagannouce-totrec
	Total Accepted	r6pagannouce-totacc
	Total Relayed	r6pagannouce-totrelay
	Total Denied	r6pagannouce-totdenied
	Total Discarded	r6pagannouce-totdiscard
	Badly Formed	r6pagannouce-badform
	Decode Error	r6pagannouce-decodeerr
	Unspecified Error	r6pagannouce-unspecerr
	Missing Mandatory TLV	r6pagannouce-missmandtlv
	TLV Value Invalid	r6pagannouce-tlvvalinval
	Unknown TLV	r6pagannouce-unknowntlv
	Duplicate TLV Found	r6pagannouce-duptlvfound
	No Session Found	r6pagannouce-nosessfound
	Admin Prohibited	r6pagannouce-admprohibit
	No Resource Drops	r6pagannouce-noresourcedrop
	Trans ID Error	r6pagannouce-transiderr
ASNPC Statistics / R6 Messages / R6 Keep Alive Request Msg	Total Received	r6keepalivereq-totrec
	Total Accepted	r6keepalivereq-totacc
	Total Relayed	r6keepalivereq-totrelay
	Total Denied	r6keepalivereq-totdenied
	Total Discarded	r6keepalivereq-totdiscard
	Badly Formed	r6keepalivereq-badform
	Decode Error	r6keepalivereq-decodeerr
	Unspecified Error	r6keepalivereq-unspecerr
	Missing Mandatory TLV	r6keepalivereq-missmandtlv
	TLV Value Invalid	r6keepalivereq-tlvvalinval
	Unknown TLV	r6keepalivereq-unknowntlv
	Duplicate TLV Found	r6keepalivereq-duptlvfound
	No Session Found	r6keepalivereq-nosessfound
	Admin Prohibited	r6keepalivereq-admprohibit
	No Resource Drops	r6keepalivereq-noresourcedrop
	Trans ID Error	r6keepalivereq-transiderr
ASNPC Statistics / R6 Messages / R6 Keep Alive Response Msg	Total Sent	r6keepaliversp-totsent
	Retransmissions Sent	r6keepaliversp-retranssent
	Total Send Failures	r6keepaliversp-totsendfail

Table 4-22 ASNPC Schema Bulk Statistic Enhancements in WEM Release 12.2

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
ASNPC Statistics / R6 Messages / R6 Unknown Messages	Total Received	r6unknown-totrec
	Total Accepted	r6unknown-totacc
	Total Relayed	r6unknown-totrelay
	Total Denied	r6unknown-totdenied
	Total Discarded	r6unknown-totdiscard
	Badly Formed	r6unknown-badform
	Decode Error	r6unknown-decodeerr
	Unspecified Error	r6unknown-unspecerr
	Missing Mandatory TLV	r6unknown-missmandtlv
	TLV Value Invalid	r6unknown-tlvvalinval
	Unknown TLV	r6unknown-unknowntlv
	Duplicate TLV Found	r6unknown-duptlvfound
	No Session Found	r6unknown-nosessfound
	Admin Prohibited	r6unknown-admprohibit
	No Resource Drops	r6unknown-noresourcedrop
	Trans ID Error	r6unknown-transiderr
ASNPC Statistics / R4 Messages / R4 Idle Mode Entry MS State Change Request Msg	Total Sent	r4imentstachareq-totsent
	Retransmissions Sent	r4imentstachareq-retranssent
	Total Send Failures	r4imentstachareq-totseTrans ID Error: ndfail
	Total Received	r4imentstachareq-totrec
	Total Accepted	r4imentstachareq-totacc
	Total Relayed	r4imentstachareq-totrelay
	Total Denied	r4imentstachareq-totdenied
	Total Discarded	r4imentstachareq-totdiscard
	Badly Formed	r4imentstachareq-badform
	Decode Error	r4imentstachareq-decodeerr
	Unspecified Error	r4imentstachareq-unspecerr
	Missing Mandatory TLV	r4imentstachareq-missmandtlv
	TLV Value Invalid	r4imentstachareq-tlvvalinval
	Unknown TLV	r4imentstachareq-unknowntlv
	Duplicate TLV Found	r4imentstachareq-duptlvfound
	No Session Found	r4imentstachareq-nosessfound
	Admin Prohibited	r4imentstachareq-admprohibit
	No Resource Drops	r4imentstachareq-noresourcedrop
	Trans ID Error	r4imentstachareq-transiderr

Table 4-22 ASNPC Schema Bulk Statistic Enhancements in WEM Release 12.2

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
ASNPC Statistics / R4 Messages / R4 Idle Mode Entry MS State Change Response Msg	Total Sent	r4imentstacharsp-totsent
	Retransmissions Sent	r4imentstacharsp-retranssent
	Total Send Failures	r4imentstacharsp-totsendfail
	Total Received	r4imentstacharsp-totrec
	Total Accepted	r4imentstacharsp-totacc
	Total Relayed	r4imentstacharsp-totrelay
	Total Denied	r4imentstacharsp-totdenied
	Total Discarded	r4imentstacharsp-totdiscard
	Badly Formed	r4imentstacharsp-badform
	Decode Error	r4imentstacharsp-decodeerr
	Unspecified Error	r4imentstacharsp-unspecerr
	Missing Mandatory TLV	r4imentstacharsp-missmandtlv
	TLV Value Invalid	r4imentstacharsp-tlvvalinval
	Unknown TLV	r4imentstacharsp-unknowntlv
	Duplicate TLV Found	r4imentstacharsp-duptlvfound
	No Session Found	r4imentstacharsp-nosessfound
	Admin Prohibited	r4imentstacharsp-admprohibit
	No Resource Drops	r4imentstacharsp-noresourcedrop
	Trans ID Error	r4imentstacharsp-transiderr
ASNPC Statistics / R4 Messages / R4 Idle Mode Entry MS State Change Ack Msg	Total Sent	r4imentstachaack-totsent
	Retransmissions Sent	r4imentstachaack-retranssent
	Total Send Failures	r4imentstachaack-totsendfail
	Total Received	r4imentstachaack-totrec
	Total Accepted	r4imentstachaack-totacc
	Total Relayed	r4imentstachaack-totrelay
	Total Denied	r4imentstachaack-totdenied
	Total Discarded	r4imentstachaack-totdiscard
	Badly Formed	r4imentstachaack-badform
	Decode Error	r4imentstachaack-decodeerr
	Unspecified Error	r4imentstachaack-unspecerr
	Missing Mandatory TLV	r4imentstachaack-missmandtlv
	TLV Value Invalid	r4imentstachaack-tlvvalinval
	Unknown TLV	r4imentstachaack-unknowntlv
	Duplicate TLV Found	r4imentstachaack-duptlvfound
	No Session Found	r4imentstachaack-nosessfound
	Admin Prohibited	r4imentstachaack-admprohibit
	No Resource Drops	r4imentstachaack-noresourcedrop
	Trans ID Error	r4imentstachaack-transiderr

Table 4-22 ASNPC Schema Bulk Statistic Enhancements in WEM Release 12.2

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
ASNPC Statistics / R4 Messages / R4 Idle Mode Exit MS State Change Request Msg	Total Sent	r4imexitstachareq-totsent
	Retransmissions Sent	r4imexitstachareq-retranssent
	Total Send Failures	r4imexitstachareq-totsendfail
	Total Received	r4imexitstachareq-totrec
	Total Accepted	r4imexitstachareq-totacc
	Total Relayed	r4imexitstachareq-totrelay
	Total Denied	r4imexitstachareq-totdenied
	Total Discarded	r4imexitstachareq-totdiscard
	Badly Formed	r4imexitstachareq-badform
	Decode Error	r4imexitstachareq-decodeerr
	Unspecified Error	r4imexitstachareq-unspecerr
	Missing Mandatory TLV	r4imexitstachareq-missmandtlv
	TLV Value Invalid	r4imexitstachareq-tlvvalinval
	Unknown TLV	r4imexitstachareq-unknowntlv
	Duplicate TLV Found	r4imexitstachareq-duptlvfound
	No Session Found	r4imexitstachareq-nosessfound
	Admin Prohibited	r4imexitstachareq-admprohibit
	No Resource Drops	r4imexitstachareq-noresourcedrop
	Trans ID Error	r4imexitstachareq-transiderr
ASNPC Statistics / R4 Messages / R4 Idle Mode Exit MS State Change Response Msg	Total Sent	r4imexitstacharsp-totsent
	Retransmissions Sent	r4imexitstacharsp-retranssent
	Total Send Failures	r4imexitstacharsp-totsendfail
	Total Received	r4imexitstacharsp-totrec
	Total Accepted	r4imexitstacharsp-totacc
	Total Relayed	r4imexitstacharsp-totrelay
	Total Denied	r4imexitstacharsp-totdenied
	Total Discarded	r4imexitstacharsp-totdiscard
	Badly Formed	r4imexitstacharsp-badform
	Decode Error	r4imexitstacharsp-decodeerr
	Unspecified Error	r4imexitstacharsp-unspecerr
	Missing Mandatory TLV	r4imexitstacharsp-missmandtlv
	TLV Value Invalid	r4imexitstacharsp-tlvvalinval
	Unknown TLV	r4imexitstacharsp-unknowntlv
	Duplicate TLV Found	r4imexitstacharsp-duptlvfound
	No Session Found	r4imexitstacharsp-nosessfound
	Admin Prohibited	r4imexitstacharsp-admprohibit
	No Resource Drops	r4imexitstacharsp-noresourcedrop
	Trans ID Error	r4imexitstacharsp-transiderr

Table 4-22 ASNPC Schema Bulk Statistic Enhancements in WEM Release 12.2

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
ASNPC Statistics / R4 Messages / R4 Initiate Paging Request Msg	Total Sent	r4inipagreq-totsent
	Retransmissions Sent	r4inipagreq-retranssent
	Total Send Failures	r4inipagreq-totsendfail
	Total Received	r4inipagreq-totrec
	Total Accepted	r4inipagreq-totacc
	Total Relayed	r4inipagreq-totrelay
	Total Denied	r4inipagreq-totdenied
	Total Discarded	r4inipagreq-totdiscard
	Badly Formed	r4inipagreq-badform
	Decode Error	r4inipagreq-decodeerr
	Unspecified Error	r4inipagreq-unspecerr
	Missing Mandatory TLV	r4inipagreq-missmandtlv
	TLV Value Invalid	r4inipagreq-tlvvalinval
	Unknown TLV	r4inipagreq-unknowntlv
	Duplicate TLV Found	r4inipagreq-duptlvfound
	No Session Found	r4inipagreq-nosessfound
	Admin Prohibited	r4inipagreq-admprohibit
	No Resource Drops	r4inipagreq-noresourcedrop
	Trans ID Error	r4inipagreq-transiderr
ASNPC Statistics / R4 Messages / R4 Initiate Paging Response Msg	Total Sent	r4inipagrsp-totsent
	Retransmissions Sent	r4inipagrsp-retranssent
	Total Send Failures	r4inipagrsp-totsendfail
	Total Received	r4inipagrsp-totrec
	Total Accepted	r4inipagrsp-totacc
	Total Relayed	r4inipagrsp-totrelay
	Total Denied	r4inipagrsp-totdenied
	Total Discarded	r4inipagrsp-totdiscard
	Badly Formed	r4inipagrsp-badform
	Decode Error	r4inipagrsp-decodeerr
	Unspecified Error	r4inipagrsp-unspecerr
	Missing Mandatory TLV	r4inipagrsp-missmandtlv
	TLV Value Invalid	r4inipagrsp-tlvvalinval
	Unknown TLV	r4inipagrsp-unknowntlv
	Duplicate TLV Found	r4inipagrsp-duptlvfound
	No Session Found	r4inipagresp-nosessfound
	Admin Prohibited	r4inipagrsp-admprohibit
	No Resource Drops	r4inipagrsp-noresourcedrop
	Trans ID Error	r4inipagrsp-transiderr

Table 4-22 ASNPC Schema Bulk Statistic Enhancements in WEM Release 12.2

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
ASNPC Statistics / R4 Messages / R4 Network Exit MS State Change Request Msg	Total Sent	r4nwexitmsstachareq-totsent
	Retransmissions Sent	r4nwexitmsstachareq-retranssent
	Total Send Failures	r4nwexitmsstachareq-totsendfail
	Total Received	r4nwexitmsstachareq-totrec
	Total Accepted	r4nwexitmsstachareq-totacc
	Total Relayed	r4nwexitmsstachareq-totrelay
	Total Denied	r4nwexitmsstachareq-totdenied
	Total Discarded	r4nwexitmsstachareq-totdiscard
	Badly Formed	r4nwexitmsstachareq-badform
	Decode Error	r4nwexitmsstachareq-decodeerr
	Unspecified Error	r4nwexitmsstachareq-unspecerr
	Missing Mandatory TLV	r4nwexitmsstachareq-missmandtlv
	TLV Value Invalid	r4nwexitmsstachareq-tlvvalinval
	Unknown TLV	r4nwexitmsstachareq-unknowntlv
	Duplicate TLV Found	r4nwexitmsstachareq-duptlvfound
	No Session Found	r4nwexitmsstachareq-nosessfound
	Admin Prohibited	r4nwexitmsstachareq-admprohibit
	No Resource Drops	r4nwexitmsstachareq-noresourcedrop
	Trans ID Error	r4nwexitmsstachareq-transiderr
ASNPC Statistics / R4 Messages / R4 Net Work Exit MS State Change Request Msg	Total Sent	r4nwexitmsstacharsp-totsent
	Retransmissions Sent	r4nwexitmsstacharsp-retranssent
	Total Send Failures	r4nwexitmsstacharsp-totsendfail
	Total Received	r4nwexitmsstacharsp-totrec
	Total Accepted	r4nwexitmsstacharsp-totacc
	Total Relayed	r4nwexitmsstacharsp-totrelay
	Total Denied	r4nwexitmsstacharsp-totdenied
	Total Discarded	r4nwexitmsstacharsp-totdiscard
	Badly Formed	r4nwexitmsstacharsp-badform
	Decode Error	r4nwexitmsstacharsp--decodeerr
	Unspecified Error	r4nwexitmsstacharsp-unspecerr
	Missing Mandatory TLV	r4nwexitmsstacharsp-missmandtlv
	TLV Value Invalid	r4nwexitmsstacharsp-tlvvalinval
	Unknown TLV	r4nwexitmsstacharsp-unknowntlv
	Duplicate TLV Found	r4nwexitmsstacharsp-duptlvfound
	No Session Found	r4nwexitmsstacharsp-nosessfound
	Admin Prohibited	r4nwexitmsstacharsp-admprohibit
	No Resource Drops	r4nwexitmsstacharsp-noresourcedrop
	Trans ID Error	r4nwexitmsstacharsp-transiderr

Table 4-22 ASNPC Schema Bulk Statistic Enhancements in WEM Release 12.2

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
ASNPC Statistics / R4 Messages / R4 Delete MS Entry Request Msg	Total Sent	r4delmsentreq-totsent
	Retransmissions Sent	r4delmsentreq-retranssent
	Total Send Failures	r4delmsentreq-totsendfail
	Total Received	r4delmsentreq-totrec
	Total Accepted	r4delmsentreq-totacc
	Total Relayed	r4delmsentreq-totrelay
	Total Denied	r4delmsentreq-totdenied
	Total Discarded	r4delmsentreq-totdiscard
	Badly Formed	r4delmsentreq-badform
	Decode Errorr4delmsentreq-tlvvalinval	r4delmsentreq-decodeerr
	Unspecified Error	r4delmsentreq-unspecerr
	Missing Mandatory TLV	r4delmsentreq-missmandtlv
	TLV Value Invalid	r4delmsentreq-tlvvalinval
	Unknown TLV	r4delmsentreq-unknowntlv
	Duplicate TLV Found	r4delmsentreq-duptlvfound
	No Session Found	r4delmsentreq-nosessfound
	Admin Prohibited	r4delmsentreq-admprohibit
	No Resource Drops	r4delmsentreq-noresourcedrop
	Trans ID Error	r4delmsentreq-transiderr
ASNPC Statistics / R4 Messages / R4 Delete MS Entry Response Msg	Total Sent	r4delmsentrsp-totsent
	Retransmissions Sent	r4delmsentrsp-retranssent
	Total Send Failures	r4delmsentrsp-totsendfail
	Total Received	r4delmsentrsp-totrec
	Total Accepted	r4delmsentrsp-totacc
	Total Relayed	r4delmsentrsp-totrelay
	Total Denied	r4delmsentrsp-totdenied
	Total Discarded	r4delmsentrsp-totdiscard
	Badly Formed	r4delmsentrsp-badform
	Decode Error	r4delmsentrsp-decodeerr
	Unspecified Error	r4delmsentrsp-unspecerr
	Missing Mandatory TLV	r4delmsentrsp-missmandtlv
	TLV Value Invalid	r4delmsentrsp-tlvvalinval
	Unknown TLV	r4delmsentrsp-unknowntlv
	Duplicate TLV Found	r4delmsentrsp-duptlvfound
	No Session Found	r4delmsentrsp-nosessfound
	Admin Prohibited	r4delmsentrsp-admprohibit
	No Resource Drops	r4delmsentrsp-noresourcedrop
	Trans ID Error	r4delmsentrsp-transiderr

Table 4-22 ASNPC Schema Bulk Statistic Enhancements in WEM Release 12.2

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
ASNPC Statistics / R4 Messages / R4 Anchor PC Ind Msg	Total Sent	r4anchorpcind-totsent
	Retransmissions Sent	r4anchorpcind-retranssent
	Total Send Failures	r4anchorpcind-totsendfail
	Total Received	r4anchorpcind-totrec
	Total Accepted	r4anchorpcind-totacc
	Total Relayed	r4anchorpcind-totrelay
	Total Denied	r4anchorpcind-totdenied
	Total Discarded	r4anchorpcind-totdiscard
	Badly Formed	r4anchorpcind-badform
	Decode Error	r4anchorpcind-decodeerr
	Unspecified Error	r4anchorpcind-unspecerr
	Missing Mandatory TLV	r4anchorpcind-missmandtlv
	TLV Value Invalid	r4anchorpcind-tlvvalinval
	Unknown TLV	r4anchorpcind-unknowntlv
	Duplicate TLV Found	r4anchorpcind-duptlvfound
	No Session Found	r4anchorpcind-nosessfound
	Admin Prohibited	r4anchorpcind-admprohibit
	No Resource Drops	r4anchorpcind-noresourcedrop
	Trans ID Error	r4anchorpcind-transiderr
ASNPC Statistics / R4 Messages / R4 Anchor PC Ack Msg	Total Sent	r4anchorpcack-totsent
	Retransmissions Sent	r4anchorpcack-retranssent
	Total Send Failures	r4anchorpcack-totsendfail
	Total Received	r4anchorpcack-totrec
	Total Accepted	r4anchorpcack-totacc
	Total Relayed	r4anchorpcack-totrelay
	Total Denied	r4anchorpcack-totdenied
	Total Discarded	r4anchorpcack-totdiscard
	Badly Formed	r4anchorpcack-badform
	Decode Error	r4anchorpcack-decodeerr
	Unspecified Error	r4anchorpcack-unspecerr
	Missing Mandatory TLV	r4anchorpcack-missmandtlv
	TLV Value Invalid	r4anchorpcack-tlvvalinval
	Unknown TLV	r4anchorpcack-unknowntlv
	Duplicate TLV Found	r4anchorpcack-duptlvfound
	No Session Found	r4anchorpcack-nosessfound
	Admin Prohibited	r4anchorpcack-admprohibit
	No Resource Drops	r4anchorpcack-noresourcedrop
	Trans ID Error	r4anchorpcack-transiderr

Table 4-22 ASNPC Schema Bulk Statistic Enhancements in WEM Release 12.2

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
ASNPC Statistics / R4 Messages / R4 Location Update Request Msg	Total Sent	r4locupdreq-totsent
	Retransmissions Sent	r4locupdreq-retranssent
	Total Send Failures	r4locupdreq-totsendfail
	Total Received	r4locupdreq-totrec
	Total Accepted	r4locupdreq-totacc
	Total Relayed	r4locupdreq-totrelay
	Total Denied	r4locupdreq-totdenied
	Total Discarded	r4locupdreq-totdiscard
	Badly Formed	r4locupdreq-badform
	Decode Error	r4locupdreq-decodeerr
	Unspecified Error	r4locupdreq-unspecerr
	Missing Mandatory TLV	r4locupdreq-missmandtlv
	TLV Value Invalid	r4locupdreq-tlvvalinval
	Unknown TLV	r4locupdreq-unknowntlv
	Duplicate TLV Found	r4locupdreq-duptlvfound
	No Session Found	r4locupdreq-nosessfound
	Admin Prohibited	r4locupdreq-admprohibit
	No Resource Drops	r4locupdreq-noresourcedrop
	Trans ID Error	r4locupdreq-transiderr
ASNPC Statistics / R4 Messages / R4 Location Update Response Msg	Total Sent	r4locupdrsp-totsent
	Retransmissions Sent	r4locupdrsp-retranssent
	Total Send Failures	r4locupdrsp-totsendfail
	Total Received	r4locupdrsp-totrec
	Total Accepted	r4locupdrsp-totacc
	Total Relayed	r4locupdrsp-totrelay
	Total Denied	r4locupdrsp-totdenied
	Total Discarded	r4locupdrsp-totdiscard
	Badly Formed	r4locupdrsp-badform
	Decode Error	r4locupdrsp-decodeerr
	Unspecified Error	r4locupdrsp-unspecerr
	Missing Mandatory TLV	r4locupdrsp-missmandtlv
	TLV Value Invalid	r4locupdrsp-tlvvalinval
	Unknown TLV	r4locupdrsp-unknowntlv
	Duplicate TLV Found	r4locupdrsp-duptlvfound
	No Session Found	r4locupdrsp-nosessfound
	Admin Prohibited	r4locupdrsp-admprohibit
	No Resource Drops	r4locupdrsp-noresourcedrop
	Trans ID Error	r4locupdrsp-transiderr

Table 4-22 ASNPC Schema Bulk Statistic Enhancements in WEM Release 12.2

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
ASNPC Statistics / R4 Messages / R4 Location Update Confirm Msg	Total Sent	r4locupdcnf-totsent
	Retransmissions Sent	r4locupdcnf-retranssent
	Total Send Failures	r4locupdcnf-totsendfail
	Total Received	r4locupdcnf-totrec
	Total Accepted	r4locupdcnf-totacc
	Total Relayed	r4locupdcnf-totrelay
	Total Denied	r4locupdcnf-totdenied
	Total Discarded	r4locupdcnf-totdiscard
	Badly Formed	r4locupdcnf-badform
	Decode Error	r4locupdcnf-decodeerr
	Unspecified Error	r4locupdcnf-unspecerr
	Missing Mandatory TLV	r4locupdcnf-missmandtlv
	TLV Value Invalid	r4locupdcnf-tlvvalinval
	Unknown TLV	r4locupdcnf-unknowntlv
	Duplicate TLV Found	r4locupdcnf-duptlvfound
	No Session Found	r4locupdcnf-nosessfound
	Admin Prohibited	r4locupdcnf-admprohibit
	No Resource Drops	r4locupdcnf-noresourcedrop
	Trans ID Error	r4locupdcnf-transiderr
ASNPC Statistics / R4 Messages / R4 PC Relocation Ind Msg	Total Sent	r4pcrelocind-totsent
	Retransmissions Sent	r4pcrelocind-retranssent
	Total Send Failures	r4pcrelocind-totsendfail
	Total Received	r4pcrelocind-totrec
	Total Accepted	r4pcrelocind-totacc
	Total Relayed	r4pcrelocind-totrelay
	Total Denied	r4pcrelocind-totdenied
	Total Discarded	r4pcrelocind-totdiscard
	Badly Formed	r4pcrelocind-badform
	Decode Error	r4pcrelocind-decodeerr
	Unspecified Error	r4pcrelocind-unspecerr
	Missing Mandatory TLV	r4pcrelocind-missmandtlv
	TLV Value Invalid	r4pcrelocind-tlvvalinval
	Unknown TLV	r4pcrelocind-unknowntlv
	Duplicate TLV Found	r4pcrelocind-duptlvfound
	No Session Found	r4pcrelocind-nosessfound
	Admin Prohibited	r4pcrelocind-admprohibit
	No Resource Drops	r4pcrelocind-noresourcedrop
	Trans ID Error	r4pcrelocind-transiderr

Table 4-22 ASNPC Schema Bulk Statistic Enhancements in WEM Release 12.2

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
ASNPC Statistics / R4 Messages / R4 PC Relocation Ack Msg	Total Sent	r4pcrelocack-totsent
	Retransmissions Sent	r4pcrelocack-retranssent
	Total Send Failures	r4pcrelocack-totsendfail
	Total Received	r4pcrelocack-totrec
	Total Accepted	r4pcrelocack-totacc
	Total Relayed	r4pcrelocack-totrelay
	Total Denied	r4pcrelocack-totdenied
	Total Discarded	r4pcrelocack-totdiscard
	Badly Formed	r4pcrelocack-badform
	Decode Error	r4pcrelocack-decodeerr
	Unspecified Error	r4pcrelocack-unspecerr
	Missing Mandatory TLV	r4pcrelocack-missmandtlv
	TLV Value Invalid	r4pcrelocack-tlvvalinval
	Unknown TLV	r4pcrelocack-unknowntlv
	Duplicate TLV Found	r4pcrelocack-duptlvfound
	No Session Found	r4pcrelocack-nosessfound
	Admin Prohibited	r4pcrelocack-admprohibit
	No Resource Drops	r4pcrelocack-noresourcedrop
	Trans ID Error	r4pcrelocack-transiderr
ASNPC Statistics / R4 Messages / R4 Context Request Msg	Total Sent	r4contextreq-totsent
	Retransmissions Sent	r4contextreq-retranssent
	Total Send Failures	r4contextreq-totsendfail
	Total Received	r4contextreq-totrec
	Total Accepted	r4contextreq-totacc
	Total Relayed	r4contextreq-totrelay
	Total Denied	r4contextreq-totdenied
	Total Discarded	r4contextreq-totdiscard
	Badly Formed	r4contextreq-badform
	Decode Error	r4contextreq-decodeerr
	Unspecified Error	r4contextreq-unspecerr
	Missing Mandatory TLV	r4contextreq-missmandtlv
	TLV Value Invalid	r4contextreq-tlvvalinval
	Unknown TLV	r4contextreq-unknowntlv
	Duplicate TLV Found	r4contextreq-duptlvfound
	No Session Found	r4contextreq-nosessfound
	Admin Prohibited	r4contextreq-adminprohib
	No Resource Drops	r4contextreq-noresourcedrop
	Trans ID Error	r4contextreq-transiderr

Table 4-22 ASNPC Schema Bulk Statistic Enhancements in WEM Release 12.2

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
ASNPC Statistics / R4 Messages / R4 Context Report Msg	Total Sent	r4contextrpt-totsent
	Retransmissions Sent	r4contextrpt-retranssent
	Total Send Failures	r4contextrpt-totsendfail
	Total Received	r4contextrpt-totrec
	Total Accepted	r4contextrpt-totacc
	Total Relayed	r4contextrpt-totrelay
	Total Denied	r4contextrpt-totdenied
	Total Discarded	r4contextrpt-totdiscard
	Badly Formed	r4contextrpt-badform
	Decode Error	r4contextrpt-decodeerr
	Unspecified Error	r4contextrpt-unspecerr
	Missing Mandatory TLV	r4contextrpt-missmandtlv
	TLV Value Invalid	r4contextrpt-tlvvalinval
	Unknown TLV	r4contextrpt-unknowntlv
	Duplicate TLV Found	r4contextrpt-duptlvfound
	No Session Found	r4contextrpt-nosessfound
	Admin Prohibited	r4contextrpt-adminprohib
	No Resource Drops	r4contextrpt-noresourcedrop
	Trans ID Error	r4contextrpt-transiderr
ASNPC Statistics / R4 Messages / R4 CMAC Key Count Update Msg	Total Sent	r4cmackeycountupd-totsent
	Retransmissions Sent	r4cmackeycountupd-retranssent
	Total Send Failures	r4cmackeycountupd-totsendfail
	Total Received	r4cmackeycountupd-totrec
	Total Accepted	r4cmackeycountupd-totacc
	Total Relayed	r4cmackeycountupd-totrelay
	Total Denied	r4cmackeycountupd-totdenied
	Total Discarded	r4cmackeycountupd-totdiscard
	Badly Formed	r4cmackeycountupd-badform
	Decode Error	r4cmackeycountupd-decodeerr
	Unspecified Error	r4cmackeycountupd-unspecerr
	Missing Mandatory TLV	r4cmackeycountupd-missmandtlv
	TLV Value Invalid	r4cmackeycountupd-tlvvalinval
	Unknown TLV	r4cmackeycountupd-unknowntlv
	Duplicate TLV Found	r4cmackeycountupd-duptlvfound
	No Session Found	r4cmackeycountupd-nosessfound
	Admin Prohibited	r4cmackeycountupd-adminprohib
	No Resource Drops	r4cmackeycountupd-noresourcedrop
	Trans ID Error	r4cmackeycountupd-transiderr

Table 4-22 ASNPC Schema Bulk Statistic Enhancements in WEM Release 12.2

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
ASNPC Statistics / R4 Messages / R4 CMAC Key Count Ack Msg	Total Sent	r4cmackeycountack-totsent
	Retransmissions Sent	r4cmackeycountack-retranssent
	Total Send Failures	r4cmackeycountack-totsendfail
	Total Received	r4cmackeycountack-totrec
	Total Accepted	r4cmackeycountack-totacc
	Total Relayed	r4cmackeycountack-totrelay
	Total Denied	r4cmackeycountack-totdenied
	Total Discarded	r4cmackeycountack-totdiscard
	Badly Formed	r4cmackeycountack-badform
	Decode Error	r4cmackeycountack-decodeerr
	Unspecified Error	r4cmackeycountack-unspecerr
	Missing Mandatory TLV	r4cmackeycountack-missmandtlv
	TLV Value Invalid	r4cmackeycountack-tlvvalinval
	Unknown TLV	r4cmackeycountack-unknowntlv
	Duplicate TLV Found	r4cmackeycountack-duptlvfound
	No Session Found	r4cmackeycountack-nosessfound
	Admin Prohibited	r4cmackeycountack-adminprohib
	No Resource Drops	r4cmackeycountack-noresourcedrop
	Trans ID Error	r4cmackeycountack-transiderr
ASNPC Statistics / R4 Messages / R4 Unknown Messages	Total Received	r4unknown-totrec
	Total Accepted	r4unknown-totacc
	Total Relayed	r4unknown-totrelay
	Total Denied	r4unknown-totdenied
	Total Discarded	r4unknown-totdiscard
	Badly Formed	r4unknown-badform
	Decode Error	r4unknown-decodeerr
	Unspecified Error	r4unknown-unspecerr
	Missing Mandatory TLV	r4unknown-missmandtlv
	TLV Value Invalid	r4unknown-tlvvalinval
	Unknown TLV	r4unknown-unknowntlv
	Duplicate TLV Found	r4unknown-duptlvfound
	No Session Found	r4unknown-nosessfound
	Admin Prohibited	r4unknown-admprohibit
	No Resource Drops	r4unknown-noresourcedrop
	Trans ID Error	r4unknown-transiderr
ASNPC Statistics / R4 Messages / General	Total Sessions Connected	total-sessions-connected
	Unknown TLV	

Web Element Manager Path

- Accounting | Bulk Statistics Configuration | Schema Tab
- Accounting | View/Graph Bulk Statistics | Select Counters and Filters Parameters Tab

CSCF Schema Bulk Statistic Enhancements

The following bulk statistics have been added to the CSCF schema in WEM Release 12.2.

Table 4-23 CSCF Schema Bulk Statistic Enhancements in WEM Release 12.2

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
CSCF Schema / CSCF Service Statistics / Calls	Mobile Originating Calls Success Rate	mo-call-succ-rate
	Mobile Terminating Calls Success Rate	mt-call-succ-rate
	Mobile Originating VOICE Calls Success Rate	mo-voice-call-succ-rate
	Mobile Terminating VOICE Calls Success Rate	mt-voice-call-succ-rate
	Mobile Originating VIDEO Calls Success Rate	mo-video-call-succ-rate
	Mobile Terminating VIDEO Calls Success Rate	mt-video-call-succ-rate
	Total Emergency Privacy Calls	emerg-priv-calls
	Total RTCP Packets Sent	rtcp-sent
	Total MSRP Packets Sent	msrp-sent
	Total MSRP Packets Received	msrp-recv
CSCF Schema / CSCF Registrations / Registration Statistics	439 FirstHopLackOb (Registration) Received	reg-resp-439rx
	439 FirstHopLackOb (Registration) Transmitted	reg-resp-439tx
CSCF Schema / CSCF Registrations / Re-Registration Statistics	439 FirstHopLackOb (Re-Registration) Received	rereg-resp-439rx
	439 FirstHopLackOb (Re-Registration) Transmitted	rereg-resp-439tx
CSCF Schema / CSCF Service Stats / CSCF Message Stats	413 Request Entity Too Large Received	message-413-rx
	413 Request Entity Too Large Transmitted	message-413-tx
CSCF Schema / SIP TCP Connection Statistics	Total TCP Subscribers	sip-tcp-subs

Table 4-23 CSCF Schema Bulk Statistic Enhancements in WEM Release 12.2

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
CSCF Schema / MSRP TCP Connection Statistics	Active Connections	msrp-active-tcp-conn
	Total Connections Closed	msrp-closed-tcp-conn
	Total Successful Outgoing Connections	msrp-succ-tcp-conn-out
	Total Failed Outgoing Connections	msrp-fail-tcp-conn-out
	Total Successful Incoming Connections	msrp-succ-tcp-conn-in
	Total Failed Incoming Connections	msrp-fail-tcp-conn-in
	Total Packets Received	msrp-packet-rx
	Total Packets Sent	msrp-packet-tx
	Total Bytes Received	msrp-bytes-rx
	Total Bytes Sent	msrp-bytes-tx
	Total MSRP Subscribers	msrp-tcp-subs
CSCF Schema / CSCF SIP Statistics / SIP Response	Received - 439 First Hop Lack Outbound	fhloerrrx
	Transmitted - 439 First Hop Lack Outbound	fhloerrtx

Table 4-23 CSCF Schema Bulk Statistic Enhancements in WEM Release 12.2

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
CSCF Schema / CSCF Statistics / CSCF Session Duration Counters	<1sec	calldur-lt-01sec
	01..10sec	calldur-01to10sec
	10..30sec	calldur-10to30sec
	30..60sec	calldur-30to60sec
	60..90sec	calldur-60to90sec
	90..120sec	calldur-90to120sec
	120..150sec	calldur-120to150sec
	150..180sec	calldur-150to180sec
	03..04min	calldur-03to04min
	04..05min	calldur-04to05min
	05..06min	calldur-05to06min
	06..07min	calldur-06to07min
	07..08min	calldur-07to08min
	08..09min	calldur-08to09min
	09..11min	calldur-09to11min
	11..13min	calldur-11to13min
	13..15min	calldur-13to15min
	15..17min	calldur-15to17min
	17..19min	calldur-17to19min
	19..21min	calldur-19to21min
	21..23min	calldur-21to23min
	23..25min	calldur-23to25min
	25..27min	calldur-25to27min
	27..29min	calldur-27to29min
	29..60min	calldur-29to60min
	>60min	calldur-gt-60min

Web Element Manager Path

- Accounting | Bulk Statistics Configuration | Schema Tab
- Accounting | View/Graph Bulk Statistics | Select Counters and Filters Parameters Tab

RP Schema Bulk Statistic Enhancements

The following bulk statistics have been added to the RP schema in WEM Release 12.2.

Table 4-24 RP Schema Bulk Statistic Enhancements in WEM Release 12.2

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
RP / Session Update Send Reason	Always On Indication	sess-always-on-indication

Web Element Manager Path

- Accounting | Bulk Statistics Configuration | Schema Tab
- Accounting | View/Graph Bulk Statistics | Select Counters and Filters Parameters Tab

CSCF-INTF Schema Bulk Statistic Enhancements

The following bulk statistics have been added to the CSCF-INTF schema in WEM Release 12.2.

Table 4-25 CSCF-INTF Schema Bulk Statistic Enhancements in WEM Release 12.2

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
CSCF_INTF / SIP Response	422 Session Interval Too Small - Received	sitserrrx
	422 Session Interval Too Small - Transmitted:	sitserrtx
	439 First Hop Lack Outbound - Received:	fhloerrrx
	439 First Hop Lack Outbound - Transmitted	fhloerrtx
CSCF_INTF / Calls	Mobile Originating Calls Success Rate	mo-call-succ-rate
	Mobile Terminating Calls Success Rate	mt-call-succ-rate
	Mobile Originating VOICE Calls Success Rate	mo-voice-call-succ-rate
	Mobile Terminating VOICE Calls Success Rate	mt-voice-call-succ-rate
	Mobile Originating VIDEO Calls Success Rate	mo-video-call-succ-rate
	Mobile Terminating VIDEO Calls Success Rate	mt-video-call-succ-rate

Web Element Manager Path

- Accounting | Bulk Statistics Configuration | Schema Tab
- Accounting | View/Graph Bulk Statistics | Select Counters and Filters Parameters Tab

Change to Threshold Description for Total HSGW Sessions

The original entry in the Online Help for this HSGW counter read:

“Configures the polling interval over which to count the forwarded packets.”

This has been corrected to: “Configures the polling interval over which to count the total number of HSGW sessions on the system.”

Web Element Manager Path

- Monitor Test Menu| Monitoring Operations Submenu | Thresholds | Descriptive Overview | Thresholds supported by the IMG

Changes in Data Values to MME Schema Bulk Statistics

The following mme bulk statistics data values have been changed from Incremental to Gauge.

Table 4-26 MME Bulk Statistic Schema Values Changed to Gauge in WEM Release 12.2

WEM Bulk Statistic Schema Directory	WEM Display Name	CLI Counter Name
MME Statistics	Attached Calls	emmcall-attach-currcall
	Maximum Calls	emmcall-attach-maxcall
	Current Calls	emmcall-connect-curcall
	Maximum Calls	emmcall-connect-maxcall
	Current Calls	emmcall-idle-curcall
	Maximum Calls	emmcall-idle-maxcall

Web Element Manager Path

On the WEM server: <*ems_dir*>/server/bsschema/mme_counter.xml

CHAPTER 5
PERFORMANCE MANAGEMENT

This chapter identifies new, modified, and obsoleted performance commands available in Release 12.0, 12.1, and 12.2.

Topics covered in this chapter are:

New Commands

This section identifies performance management commands that are new in Release 12.x.

Common Commands - New in Release 12.0

The following common commands are new in Release 12.0.

monitor diameter

This command enables SRP monitoring of the connection between the specified Diameter server and the primary chassis.

CLI (Service Redundancy Protocol Configuration Mode)

[no] monitor diameter context *context_name* **endpoint** *endpoint_name* **[fqdn** *fqdn* **| peer {** *IPv4_address* **|** *IPv6_address* **}] [port** *port_number* **]**

show tacacs

Provides TACACS+ configuration and session state information for each active TACACS+ session.

CLI (Exec Mode)

show tacacs

show tacacs client statistics

Provides system-wide client statistics for all TACACS+ sessions.

CLI (Exec Mode)

```
show tacacs client statistics
```

show tacacs session statistics

Provides system-wide session statistics, including protocol statistics, for active TACACS+ sessions.

CLI (Exec Mode)

```
show tacacs session statistics
```

Common Commands - New in Release 12.2

The following common commands are new in Release 12.2.

clear srp

This command clears system Service Redundancy Protocol (SRP) statistics.

CLI (Exec Mode)

```
clear srp { audit-statistics | call-loss statistics | checkpoint statistics
| statistics }
```

threshold aaa-acct-archive-queue

This command configures accounting message archive queue size threshold for generating alerts or alarms based on the archive queue percentage of AAA accounting messages in the buffer during the polling interval.

CLI (Global Configuration Mode)

```
threshold aaa-acct-archive-queue-size1 high_thresh [ clear low_thresh ]
threshold aaa-acct-archive-queue-size2 high_thresh [ clear low_thresh ]
threshold aaa-acct-archive-queue-size3 high_thresh [ clear low_thresh ]
default threshold aaa-acct-archive-queue-size1
default threshold aaa-acct-archive-queue-size2
default threshold aaa-acct-archive-queue-size3
```

threshold monitoring aaa-acct-archive-queue

This command enables/disables threshold monitoring for accounting message archive queue size thresholds.

CLI (Global Configuration Mode)

```
threshold monitoring aaa-acct-archive-queue
default threshold monitoring aaa-acct-archive-queue
```

threshold poll aaa-acct-archive-queue

This command configures the polling interval for accounting message archive queue size thresholds.

CLI (Global Configuration Mode)

```
threshold poll aaa-acct-archive-queue-size1 interval time
threshold poll aaa-acct-archive-queue-size2 interval time
threshold poll aaa-acct-archive-queue-size3 interval time
default threshold poll aaa-acct-archive-queue-size1 interval
default threshold poll aaa-acct-archive-queue-size2 interval
default threshold poll aaa-acct-archive-queue-size3 interval
```

accept-zero-as-rd

This command configures to accept VPN prefixes with Router Distinguisher (RD) value having Administrator Subfield, which is an Autonomous System number 0.

CLI (BGP Configuration Mode)

```
[no] accept-zero-as-rd
```

Application Detection and Control - New in Release 12.0

The following Application Detection and Control commands are new in Release 12.0.

None for this release.

Content Filtering Commands - New in Release 12.0

The following Content Filtering commands are new in Release 12.0.

None for this release.

ECS Commands - New in Release 12.0

The following ECS commands are new in Release 12.0.

None for this release.

ECS Commands - New in Release 12.2

The following ECS commands are new in Release 12.2.

clear active-charging dns-learnt-ip-addresses

This command clears DNS learnt IP address statistics for the DNS Snooping feature.

CLI (Exec Mode)

clear active-charging dns-learnt-ip-addresses statistics sessmgr { all | instance *sessmgr_instance* **} [| { grep** *grep_options* **| more }]**

clear active-charging tethering-detection statistics

This command clears statistics pertaining to the Tethering Detection feature.

CLI (Exec Mode)

clear active-charging tethering-detection statistics

show active-charging dns-learnt-ip-addresses

This command displays DNS learnt IP address statistics for the DNS Snooping feature.

CLI (Exec Mode)

show active-charging dns-learnt-ip-addresses statistics { sessmgr { all | instance *sessmgr_instance* **} [verbose] | summary } [| { grep** *grep_options* **| more }]**

show active-charging tethering-detection

This command displays information/statistics pertaining to Tethering Detection databases.

CLI (Exec Mode)

show active-charging tethering-detection { database [os-signature | tac | ua-signature]+ [sessmgr { all | instance *instance* **}] [| { grep** *grep_options* **| more }] | statistics }**

Firewall Commands - New in Release 12.0

The following Stateful Firewall commands are new in Release 12.0.

None for this release.

GGSN Commands - New in Release 12.0

The following GGSN commands are new in Release 12.0.

None for this release.

HA Commands - New in Release 12.0

The following HA commands are new in Release 12.0.

None for this release.

IPCF Commands - New in Release 12.1

This section provides information on new IPCF commands available in Release 12.1.

IPCF is new product for this release.

Command Line Interface

Exec Mode Commands

- clear event-notif server
- clear event-notif statistics
- clear pcc-af service
- clear pcc-af session
- clear pcc-policy service statistics
- clear pcc-policy session
- clear pcc-service
- clear pcc-sp-endpoint statistics
- show event-notif server
- show event-notif statistics
- show pcc-af service
- show pcc-af session
- show pcc-policy service
- show pcc-policy session
- show pcc-service
- show pcc-service session
- show pcc-service statistics
- show pcc-sp-endpoint
- show pcc-sp-endpoint connection

Mobility Management Entity Commands - New in Release 12.0

The following Mobility Management Entity (MME) commands are new in Release 12.0.

show lte-policy

The **`show lte-policy`** command is new in release 12.0 and is a direct replacement for the obsolete command **`show mme-policy`**.

CLI (Exec Mode)

`show lte-policy { ho-restriction-list { name` *`name`* **| `subscriber-map { name`** *`name`* **| `summary } | tai-mgmt-db { name`** *`name`* **| `summary }} [ | { grep`** *`grep_options`* **| `more } ]`**

show sctp-param-template

The **show sctp-param-template** command is new in release 12.0. The output of this command displays configuration information for SCTP parameter templates configured on the system.

CLI (Exec Mode)

show sctp-param-template { all | name *temlate_name* **} { | grep** *grep_options* **| more }]**

Mobility Management Entity Commands - New in Release 12.2

The following Mobility Management Entity (MME) commands are new in Release 12.2.

show ip traffic sctp card

The **show iptraffic sctp** command displays kernel traffic information for Stream Control Traffic Protocol. The card slot number and CPU number must be specified.

CLI (Exec Mode)

show ip traffic sctp card *card_number* **cpu** *cpu_number*

show sgs-service offload-status service-name

This command displays VLR offload information and statistics for the specified SGs service.

CLI (Exec Mode)

show sgs-service offload-status service-name *sgs_svc_name*

NAT Commands - New in Release 12.0

The following NAT commands are new in Release 12.0.

show active-charging analyzer statistics name h323 verbose

This command displays active charging protocol analyzer statistics for H323 analyzer. The output of this command includes the following new fields:

- H323 Session Stats
  - Total Uplink Bytes
  - Total Downlink Bytes
  - Total Uplink Packets
  - Total Downlink Packets
  - Total H323 calls
  - Total RAS messages
  - Total Q931 messages
  - Total H245 messages
- RAS messages
  - GatekeeperRequest

    - GatekefeperConfirm
    - GatekeeperReject
    - RegistrationRequest
    - RegistrationConfirm
    - RegistrationReject
    - UnregistrationRequest
    - UnregistrationConfirm
    - AdmissionRequest
    - UnregistrationReject
    - AdmissionRequest
    - AdmissionConfirm
    - AdmissionReject
    - LocationRequest
    - LocationConfirm
    - LocationReject
    - DisengageRequest
    - DisengageConfirm
    - DisengageReject
    - InfoRequest
    - InfoRequestResponse
    - RequestInProgress
    - Unclassified
  - Q931 messages
    - Alerting
    - CallProceeding
    - Setup
    - Connect
    - ReleaseComplete
    - Facility
    - Progress
    - Information
    - Unclassified
  - H245 messages
    - OpenLogicalChannel
    - OpenLogicalChannelAck
    - OpenLogicalChannelReject
    - OpenLogicalChannelConfirm
    - RequestChannelClose

- CloseLogicalChannel
- CloseLogicalChannelAck
- EndSessionCommand
- Unclassified

CLI (Exec Mode)

show active-charging analyzer statistics name h323 [verbose]] [| { grep *grep_options* **| more }]**

Packet Data Network Gateway Commands - New in Release 12.0

This section provides information on new P-GW commands available in Release 12.0.

clear local-policy

Clears local QoS policy service statistics and counters found in show command outputs and bulk statistics associated with all local QoS policy services or a specific service defined by the parameter in this command.

CLI (Exec Mode)

clear local-policy statistics [service *service_name* **]**

PDIF Commands - New in Release 12.0

The following PDIF commands are new in Release 12.0.

None for this release.

PDSN Commands - New in Release 12.0

The following PDSN commands are new in Release 12.0.

None for this release.

Serving Gateway Commands - New in Release 12.0

The following commands are new in Release 12.0.

show lte-policy

The **show lte-policy** command is new in release 12.0 and is a direct replacement for the obsolete command **show mme-policy**. The S-GW now supports commands in the LTE Policy Configuration Mode.

CLI (Exec Mode)

show lte-policy { ho-restriction-list { name *name* **| subscriber-map { name** *name* **| summary } | tai-mgmt-db { name** *name* **| summary } } [| { grep** *grep_options* **| more }]**

Serving Gateway Commands - New in Release 12.2

The following command is new in Release 12.2.

accounting mode

The **accounting mode** command is new in release 12.2 The S-GW now supports accounting via GTPP (default), RADIUS/Diameter or None.

CLI (S-GW Service Configuration Mode)

[default] accounting mode { gtpp | none| radius-diameter }

Session Control Manager Commands - New in Release 12.2

The following SCM commands are new in Release 12.2.

show cscf ifc

Displays configured iFC in XML format, as per 3GPP TS 29.228 Annex E, for CSCF services on this system.

CLI (Exec Mode)

show cscf ifc { all | id *id* **} [| { grep** *grep_options* **| more }]**

show cscf npdb-servers

Displays connection status of NPDB (Number Portability Data Base) server in S-CSCF service.

CLI (Exec Mode)

show cscf npdb-servers service *service_name*

EXAMPLE(S)

```
[local]asr5000# show cscf npdb-servers service <service_name>
-----------------------------------------------------------------------
Context :  v4scscf   Service  :  v4scscf
Client : npdb-client   Address : 192.168.1.1
Req ID  :   lgt
-----------------------------------------------------------------------

Smgr-ID   Client-ID    Type      State           Peer Address
======    =======      ====      ===========     ==============
  1       10021        PRI       OPEN [TCP]      192.168.50.1:3868
  1       10021        SEC       OPEN [NPDB]     192.168.70.1:3878
200       10230        PRI       IDLE            192.168.50.1:3868
150       10170        PRI       PROGRESS        192.168.50.1:3868
100       10120        PRI       IDLE            192.168.50.1:3868

Peers Summary:
  Peers in IDLE state: 2
  Peers in OPEN state: 2
  Peers in PROGRESS: 1
```

```
Total peers matching specified criteria: 5
```

SGSN Commands - New in Release 12.0

The following SGSN commands are new in Release 12.0.

clear sgsn-pool statistics

The following command clears statistics collected for monitoring the number of subscribers offloaded to a target NRI.

CLI (Exec Mode)

clear sgsn-pool statistics { gprs-service <*service_name*> | sgsn-service <*service_name*> } { nri-value <*a - 63*> | peer-non-broadcast-lac <*1 - 65535*> rac <*0 - 255*> | target-offloaded-to-peer [target-nri *<0 - 63*>] }

show linecard dlci-utilization

The following command is new in this release to track DLCI utilization per CLC-type line card:

CLI (Exec Mode)

show linecard dlci-utilization *card#* **[| { grep grep_options | more }]**

The output for this command includes the fields listed below:

- Port
- Path
- E1T1
- TS
- DLCI
- NSE
- NSVC
- Average DLCI Utilization (in kbps)
- Current Rx
- Current Tx
- 5min Rx
- 5min Tx
- 15min Rx
- 15min Tx

show sgsn-pool statistics

The following command displays statistics collected for monitoring the number of subscribers offloaded to a target NRI.

CLI (Exec Mode)

show sgsn-pool statistics { gprs-service <*service_name*> | sgsn-service <*service_name*> } { nri-value <*0 - 63*> | peer-non-broadcast-lac <*1 - 65535*> rac <*0 - 255*> | target-load-in-progress [smgr-instance <*1 - 230*> | target-nri <*0 - 63*>] | target-offloaded-to-peer [target-nri <*0 - 63*>] }

Modified Commands

This section identifies performance management commands modified in Release 12.x.

Common Commands - Modified in Release 12.0

The following common commands have been modified in Release 12.0.

clear dns-client

The **clear dns-client** command has two new **query-type** keywords in release 12.0: **AAAA** and **NAPTR**. These keywords clear filtered DNS results based on 128-bit domain IPv6 addresses (AAAA resource records) or on Naming Authority Pointer records (NAPTR).

CLI (Exec Mode)

clear dns-client *name* **{ cache client** *name* **[query-name** *name* **| query-type { A | AAAA | NAPTR | SRV }] | statistics }**

logging filter active facility

The **logging filter active facility** command adds the ability to generate logging outputs for the following seven facilities in release 12.0: **callhome**, **epdg**, **lagmgr**, **phs**, **pppoe**, **testctrl**, and **testmgr**.

The following facility is no longer in the **logging filter active facility** command in release 12.0: **event-notif**.

CLI (Exec Mode)

logging filter active facility *facility*

logging filter runtime facility

The **logging filter runtime facility** command adds the ability to generate logging outputs for the following seven facilities in release 12.0: **callhome**, **epdg**, **lagmgr**, **phs**, **pppoe**, **testctrl**, and **testmgr**.

The following facility is no longer in the **logging filter runtime facility** command in release 12.0: **event-notif**.

CLI (Global Configuration Mode)

logging filter runtime facility *facility*

monitor protocol

The **monitor protocol** command adds the ability to monitor four new protocols in release 12.0: SSCOP, SSCFNNI, PHS (Payload Header Suppression), and PPPOE.

CLI (Exec Mode)

monitor protocol

save logs facility

The **save logs facility** command adds the ability to save logging outputs for the following seven facilities in release 12.0: **callhome**, **epdg**, **lagmgr**, **phs**, **pppoe**, **testctrl**, and **testmgr**.

The following facility is no longer in the **save logs facility** command in release 12.0: **event-notif**.

CLI (Exec Mode)

save logs facility *facility*

show aaa group name

This command is used to view AAA statistics for the current context. The output of this command includes a new field “Fire-and-Forget” to display whether or not the Fire-And-Forget feature is enabled in the AAA Group configuration.

In addition, the following fields have been added under **`Attributes`** to indicate whether or not RADIUS accounting and authentication attributes have been enabled. The attributes must also be supported in the configured RADIUS dictionary.

- Authentication
  - called-station-id
  - calling-station-id
  - imsi
  - 3gpp-pdp-type
  - 3gpp-cg-address
  - 3gpp-gprs-qos-negotiated-profile
  - 3gpp-sgsn-address
  - 3gpp-ggsn-address
  - 3gpp-imsi-mcc-mnc
  - 3gpp-ggsn-mcc-mnc
  - 3gpp-nsapi
  - 3gpp-select-mode
  - 3gpp-charging-characteristics
  - 3gpp-sgsn-mcc-mnc
  - 3gpp-imeisv
  - 3gpp-rat-type
  - 3gpp-user-location-info
  - 3gpp-ms-timezone
- Accounting
  - called-station-id
  - calling-station-id
  - acct-input-octets
  - acct-input-packets
  - acct-session-time
  - acct-output-octets
  - acct-output-packets
  - event-timestamp
  - imsi
  - 3gpp-charging-id
  - 3gpp-pdp-type

- 3gpp-cg-address
- 3gpp-gprs-qos-negotiated-profile
- 3gpp-sgsn-address
- 3gpp-ggsn-address
- 3gpp-imsi-mcc-mnc
- 3gpp-ggsn-mcc-mnc
- 3gpp-nsapi
- 3gpp-select-mode
- 3gpp-charging-characteristics
- 3gpp-sgsn-mcc-mnc
- 3gpp-imeisv
- 3gpp-rat-type
- 3gpp-user-location-info
- 3gpp-ms-timezone

CLI (Exec Mode)

show aaa { group { all | name *aaa_group_name* **} | local counters } [| { grep** *grep_options* **| more }]**

show active-charging analyzer statistics name pptp

This command displays active charging protocol analyzer statistics for the PPTP analyzer. The output of this command includes the following new fields to display PPTP-GRE traffic statistics:

- ACS PPTP-GRE Session Stats
  - Total Uplink Bytes
  - Total Downlink Bytes
  - Total Uplink Pkts
  - Total Downlink Pkts

CLI (Exec Mode)

show active-charging analyzer statistics name sip [verbose]] [| { grep *grep_options* **| more }]**

show active-charging flows type p2p

This command displays active charging protocol analyzer statistics for the PPTP analyzer. The following data transport protocols are added:

- (I) - ICMP and ICMPv6
- (G) - GREv1

CLI (Exec Mode)

show active-charging flows { all | [connected-time [< | > | greater-than | less-than] *seconds* **] [flow-id** *flow_id* **] [full] [idle-time [< | > | greater-than | less-than]** *seconds* **] [ip-address [server | subscriber] [**

< | > | IPv4 | greater-than | less-than] *address* **] [nat { not-required | required [nat-ip** *nat_ip_address* **] }] [port-number [server | subscriber] [< | > | IPv4 | greater-than | less-than]** *number* **] [rx-bytes [< | > | greater-than | less-than]** *number* **] [rx-packets [< | > | greater-than | less-than]** *number* **] [session-id** *session_id* **] [summary] [trans-proto { icmp | tcp | udp }] [tx-bytes [< | > | greater-than | less-than]** *number* **] [tx-packets [< | > | greater-than | less-than]** *number* **] [type** *flow_type* **] } [| { grep** *grep_options* **| more }]**

show active-charging service all

This command displays ACS service details. The output of this command includes the following new fields:

- Server Unreachable Failure-Handling
  - Initial-Request
  - Update-Request

CLI (Exec Mode)

show active-charging service { all | name *service_name* **} [| { grep** *grep_options* **| more }]**

show active-charging sessions

This command displays active charging statistics for ACS sessions. The output of the following commands includes the new field “Current PPTP-GRE Sessions”.

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

CLI (Exec Mode)

show active-charging sessions [full [wide] | summary | display-dynamic-charging-rules | dynamic-charging] { [all] | [*filter_keyword* **] + } [| { grep** *grep_options* **| more }]**

show active-charging sessions full

This command displays active charging statistics for ACS sessions. The output of this command includes the following new field:

- Current PPTP-GRE Flows

CLI (Exec Mode)

show active-charging sessions [full [wide] | summary | display-dynamic-charging-rules | dynamic-charging] { [all] | [*filter_keyword* **] + } [| { grep** *grep_options* **| more }]**

show active-charging sessions full all

This command displays ACS session statistics. The output of this command includes the following new fields:

- CCR-I Server Unreachable Handling
- CCR-U Server Unreachable Handling

CLI (Exec Mode)

show active-charging sessions [full [wide] | summary | display-dynamic charging-rules | dynamic-charging] { [all] | [*filter_keyword*] + } [| { grep *grep_options* | more }]

show active-charging subsystem all

This command displays active statistics for ACS sessions. The output of this command includes the following new fields:

- Total PPTP-GRE flows
- Current PPTP-GRE flows

CLI (Exec Mode)

show active-charging subsystem { all | facility acsmgr { all | instance *instance_value* **} [rulebase name** *rulebase_name* **] | sip } [| { grep** *grep_options* **| more }]**

show apn name

This command is used to display configuration information for either a specific or all configured APNs. The output of this command includes the following new fields:

- Radius Secondary Group — to indicate the secondary Accounting group configured in the APN configuration.
- Accounting Policy Name — to indicate the name of accounting policy associated with the APN.

CLI (Exec Mode)

show apn { all | name *apn_name* **} [| { grep** *grep_options* **| more }]**

show apn statistics

This command is used to display statistics for either a specific Access Point Name (APN) or all configured APNs. The description has changed for the output field **Current APN context load**.

Previous Behavior: The current percent utilization of the APN as function of the APN's configured maximum number of supported PDP contexts and the current total number of PDP contexts facilitated by the APN.

New Behavior: Current APN context load = (current contexts (selected APN(s)) / current contexts (system wide)) * 100.

CLI (Exec Mode)

show apn statistics { all | name *apn_name* **} [| { grep** *grep_options* **| more }]**

show diameter route table

This command displays the Diameter routing table. The output of this command has been modified to display the dynamic routes with a flag 'D'.

CLI (Exec Mode)

show diameter route table [wide] [endpoint *endpoint_name* **] [| { grep** *grep_options* **| more }]**

show diameter statistics

This command displays the Diameter peer statistics. The output of this command includes the following new fields.

- Dynamic Route statistics
  - Adds
  - Add Failures
  - Removes
  - Hits
  - Expires

CLI (Exec Mode)

show diameter statistics [[proxy] | endpoint *endpoint_name* **[peer-host** *peer_id* **[peer-realm** *realm_id* **]]] [| { grep** *grep_options* **| more }]**

show dns-client

The **show dns-client** command has two new **query-type** keywords in release 12.0: **AAAA** and **NAPTR**. These keywords filter DNS results based on 128-bit domain IPv6 addresses (AAAA resource records) or on Naming Authority Pointer records (NAPTR).

CLI (Exec Mode)

show dns-client { cache client *name* **[query-name** *name* **| query-type { A | AAAA | NAPTR | SRV }] | statistics client** *name* **} [| { grep** *grep_options* **| more }]**

show gtpc statistics

This command displays the GTPC statistics. The output of this command includes the following new fields:

- current-ipv4v6
- setup-ipv4v6
- dyn-ipv4v6

CLI (Exec Mode)

show gtpc statistics [verbose]

show ims-authorization policy-control statistics server

Displays information and statistics specific to the policy control in IP Multimedia Subsystem (IMS) authorization service. This command has been enhanced to display IPv6 address in addition to IPv4 address in Release 12.0.

CLI (Exec Mode)

show ims-authorization policy-control statistics [service *ims_auth_svc_name* **| server { ip-address** *ip_address* **[port** *port_value* **] | name** *server_name* **}] [| { grep** *grep_options* **| more }]**

show logs facility

The **show logs facility** command adds the ability to display logging outputs for the following seven facilities in release 12.0: **callhome**, **epdg**, **lagmgr**, **phs**, **pppoe**, **testctrl**, and **testmgr**.

The following facility is no longer in the **show logs facility** command in release 12.0: **event-notif**.

CLI (Exec Mode)

show logs facility *facility*

show session subsystem facility aaamgr

Shows information for subscriber sessions defined by the specified keywords. The output of this command includes the following new fields to track the number of secondary accounting requests in the AAAMgr instance.

- Total radius sec acct requests
- Current radius sec acct requests
- Total radius sec acct cancelled
- Total radius sec acct purged
- Total radius sec acct requests retried

CLI (Exec Mode)

show session subsystem facility aaamgr { all | instance | verbose } [| { grep *grep_options* **| more }]**

show srp

This command displays the Service Redundancy Protocol information. The following keywords have been added to this command:

- **active**
- **standby**
- **diameter**

CLI (Exec Mode)

show srp { call-loss statistics | checkpoint statistics [active | standby] [verbose] | info | monitor [all | authentication-probe | bgp | diameter] | statistics } | [grep *grep_options* **| more]**

show subscribers configuration username

Shows information for subscriber sessions defined by the specified keywords. The output of this command includes a new field “Radius Secondary Group” to indicate the secondary Accounting group configured in the Subscriber configuration.

CLI (Exec Mode)

show subscribers configuration { all | username *user_name* **} [| { grep** *grep_options* **| more }]**

show subscribers full all

Shows information for subscriber sessions defined by the specified keywords. The output of this command includes a new field “AAA Radius Secondary group” to indicate the secondary Accounting group configured in the Subscriber configuration.

CLI (Exec Mode)

show subscribers full all [| { grep *grep_options* **| more }]**

Common Commands - Modified in Release 12.2

The following common commands have been modified in Release 12.2.

clear active-charging ruledef statistics

This command clears statistics for rule definitions configured in the Active Charging Service (ACS). The tpo option was added to this command, which enables to clear statistics for Traffic Performance Optimization (TPO) ruledefs configured in the ACS.

CLI (Exec Mode)

clear active-charging ruledef statistics [charging | firewall | name *ruledef_name* **| tpo] [| { grep** *grep_options* **| more }]**

monitor protocol

This command enters the system‘s protocol monitoring utility. The following protocols have been added to this utility:

- **RTP (IMS)**
- **RTCP (IMS)**

CLI (Exec Mode)

monitor protocol

show active-charging credit-control session-states

This command displays statistics for Diameter/RADIUS Prepaid Credit Control Service in the Active Charging Service (ACS). A new field "Backpressured" has been added to the output of this command to display backpressure condition in credit-control sessions.

CLI (Exec Mode)

show active-charging credit-control { statistics [all | group *group_name* **] | session-states [rulebase** *rulebase_name* **] [content-id** *content_id* **] } [| { grep** *grep_options* **| more }]**

show active-charging ruledef

This command displays information/statistics for rule definitions (ruledefs) configured in the Active Charging Service (ACS). The **tpo** option was added to this command, which enables to view information/statistics for all TPO ruledefs configured in the ACS.

CLI (Exec Mode)

show active-charging ruledef { all | charging | firewall | name *ruledef_name* **| post-processing | routing | statistics [all { charging | firewall [wide] | post-processing | tpo } | name** *ruledef_name* **[wide]] | tpo } [| { grep** *grep_options* **| more }]**

show active-charging service all

This command displays active charging protocol analyzer statistics for the PPTP analyzer. The output of this command includes the following new fields to display PPTP-GRE traffic statistics:

- MSISDN-Range-Mode
- MSISDN-Based End-Value
- MSISDN-Based Start-Value

CLI (Exec Mode)

show active-charging service { all | name acs_service_name } [| { grep *grep_options* **| more }]**

show active-charging sessions full

This command displays statistics for Active Charging Service (ACS) sessions. A new field "Backpressured" has been added to the output of this command to display backpressure condition in credit-control sessions.

CLI (Exec Mode)

show active-charging sessions [full [wide] | summary | display-dynamic-charging-rules | dynamic-charging] { [all] | [*filter_keyword* **] + } [| { grep** *grep_options* **| more }]**

show active-charging sessions

This command displays statistics for Active Charging Service (ACS) sessions. The output of this command includes the following new fields to display the maximum number of simultaneous L3 flows seen by the session and the time at which they were observed:

- Max (L3) Flows
- Max Flows Timestamp

CLI (Exec Mode)

show active-charging session full all

show active-charging subsystem

This command displays service and configuration counters for the ACS. The output of this command includes the following new fields to display the maximum number of simultaneous flows seen per session:

- Max flows per-session Statistics:
  - Max Flows seen
  - IMSI
  - Max Flows seen at

CLI (Exec Mode)

show active-charging subsystem facility acsmgr instance *instance_value*

show gtpp group

This command displays information pertaining to the configured GTPP storage server group. The output of this command includes a new field "**ULI-Change**" to display whether or not the uli-change triggers are configured.

CLI (Exec Mode)

show gtpp group [name *gtpp_group_name* **| all] [| { grep** *grep_options* **| more }]**

show ims-authorization service statistics

This command displays information, configuration, and statistics of all/specific IP Multimedia Subsystem (IMS) authorization service. A new counter "Resource Modification Req" has been added to the output of this command.

CLI (Exec Mode)

show ims-authorization service { { all [verbose] | name *ims_auth_svc_name* **| summary] } | { statistics [all | name** *ims_auth_svc_name* **] [verbose] } [| { grep** *grep_options* **| more }]**

show srp

This command displays Service Redundancy Protocol (SRP) related information.

The ability to display statistics of external audit has been added to this command.

For Traffic Performance Optimization (TPO) ICSR support, the output of the following commands include the new field "tpo-policy-mapping-id failures", which indicates the number of TPO policy ID mapping failures in the standby Session Manager.

- **show srp checkpoint statistics**
- **show srp checkpoint statistics sessmgr [all | instance]** — this is a hidden CLI command
- **show srp checkpoint statistics standby verbose**
- **show srp checkpoint statistics standby debug-info verbose** — this is a hidden CLI command

CLI (Exec Mode)

show srp { audit-statistics [all | instance *number* **] [message-level | session-level] | call-loss statistics | checkpoint statistics [active | standby] [verbose] | info | monitor [all | authentication-probe | bgp | diameter] | statistics } | [grep** *grep_options* **| more]**

show task

New **memory** keyword. displays detailed task memory use information.

CLI (Exec Mode)

show task { info | memory | resources | table } [card *card_num* **] [facility** *facility* **{ all | instance** *id* **}] [process** *process_name* **all] [max] [| { grep** *grep_options* **| more }]**

Application Detection and Control Commands - Modified in Release 12.0

The following commands have been modified in Release 12.0.

clear active-charging analyzer statistics

This command supports the clearing of protocol analyzer statistics for the following P2P applications:

- blackberry
- gmail
- itunes
- myspace
- teamviewer
- twitter
- viber

CLI (Exec Mode)

clear active-charging charging-action statistics [name *string* **] [| { grep** *grep_options* **| more }]**

show active-charging analyzer statistics name p2p verbose

This command displays Active Charging protocol analyzer statistics for the P2P protocol analyzer. The output of this command includes the following new fields to display the uplink/downlink bytes and uplink/downlink packets for the following protocols:

- Blackberry
- Gmail
- iTunes
- MySpace
- TeamViewer
- Twitter
- Viber
- Yahoo-video
- Oscar-video
- Gtalk-video

CLI (Exec Mode)

show active-charging analyzer statistics name p2p [verbose] [| { grep *grep_options* **| more }]**

show active-charging flows

This command displays the information for the active charging flows. The P2P protocol type flows now support the following applications:

- blackberry
- gmail
- itunes
- myspace
- teamviewer
- twitter
- viber

CLI (Exec Mode)

show active-charging flows { all | [connected-time [< | > | greater-than | less-than] *seconds*] [flow-id *flow_id*] [full] [idle-time [< | > | greater-than | less-than] *seconds*] [ip-address [server | subscriber] [< | > | IPv4 | greater-than | less-than] *address*] [nat { not-required | required [nat-ip *nat_ip_address*] }] [port-number [server | subscriber] [< | > | IPv4 | greater-than | less-than] *number*] [rx-bytes [< | > | greater-than | less-than] *number*] [rx-packets [< | > | greater-than | less-than] *number*] [session-id *session_id*] [summary] [trans-proto { icmp | tcp | udp }] [tx-bytes [< | > | greater-than | less-than] *number*] [tx-packets [< | > | greater-than | less-than] *number*] [type *flow_type*] } [| { grep *grep_options* | more }]

show active-charging sessions

This command displays statistics for ACS sessions. The P2P protocol type flows now support the following applications:

- blackberry
- gmail
- itunes
- myspace
- teamviewer
- twitter
- viber

CLI (Exec Mode)

show active-charging sessions [full [wide] | summary | display-dynamic-charging-rules | dynamic-charging] { [all] | [*filter_keyword*] + } [| { grep *grep_options* | more }]

show active-charging sessions summary

This command displays statistics for specific active charging service sessions. The output of this command includes the following new fields:

- Current BLACKBERRY Sessions

- Current GMAIL Sessions
- Current ITUNES Sessions
- Current MYSPACE Sessions
- Current TEAMVIEWER Sessions
- Current TWITTER Sessions
- Current VIBER Sessions
- Current YAHOO Video Sessions
- Current OSCAR Video Sessions
- Current GTALK Video Sessions

CLI (Exec Mode)

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

show active-charging sessions summary type p2p

This command displays summary information for P2P active charging service sessions. The output of this command includes the following new fields:

- Current BLACKBERRY Sessions
- Current GMAIL Sessions
- Current ITUNES Sessions
- Current MYSPACE Sessions
- Current TEAMVIEWER Sessions
- Current TWITTER Sessions
- Current VIBER Sessions
- Current YAHOO Video Sessions
- Current OSCAR Video Sessions
- Current GTALK Video Sessions

CLI (Exec Mode)

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

Application Detection and Control Commands - Modified in Release 12.2

The following commands have been modified in Release 12.2.

clear active-charging analyzer statistics

This command supports the clearing of protocol analyzer statistics for the following P2P applications:

- antsp2p

- imo
- mypeople
- netmotion
- ogg
- openvpn
- quicktime
- rdt
- scydo
- spotify
- tango
- tunnelvoice
- ultrabac
- usenet
- whatsapp

CLI (Exec Mode)

clear active-charging charging-action statistics [name *string* **] [| { grep** *grep_options* **| more }]**

show active-charging analyzer statistics name p2p verbose

This command displays Active Charging protocol analyzer statistics for the P2P protocol analyzer. The output of this command includes the following new fields to display the uplink/downlink bytes and uplink/downlink packets for the following protocols:

- AntsP2P
- IMO
- MyPeople
- Netmotion
- OGG
- OpenVPN
- Quicktime
- RDT
- Scydo
- Spotify
- Tango
- TunnelVoice
- Ultrabac
- Usenet
- WhatsApp

CLI (Exec Mode)

show active-charging analyzer statistics name p2p [verbose] [| { grep *grep_options* **| more }]**

show active-charging flows

This command displays the information for the active charging flows. The P2P protocol type flows now support the following applications:

- antsp2p
- imo
- mypeople
- netmotion
- ogg
- openvpn
- quicktime
- rdt
- scydo
- spotify
- tango
- tunnelvoice
- ultrabac
- usenet
- whatsapp

CLI (Exec Mode)

show active-charging flows { all | [connected-time [< | > | greater-than | less-than] *seconds* **] [flow-id** *flow_id* **] [full] [idle-time [< | > | greater-than | less-than]** *seconds* **] [ip-address [server | subscriber] [< | > | IPv4 | greater-than | less-than]** *address* **] [nat { not-required | required [nat-ip** *nat_ip_address* **] }] [port-number [server | subscriber] [< | > | IPv4 | greater-than | less-than]** *number* **] [rx-bytes [< | > | greater-than | less-than]** *number* **] [rx-packets [< | > | greater-than | less-than]** *number* **] [session-id** *session_id* **] [summary] [trans-proto { icmp | tcp | udp }] [tx-bytes [< | > | greater-than | less-than]** *number* **] [tx-packets [< | > | greater-than | less-than]** *number* **] [type** *flow_type* **] } [| { grep** *grep_options* **| more }]**

show active-charging sessions

This command displays statistics for ACS sessions. The P2P protocol type flows now support the following applications:

- antsp2p
- imo
- mypeople
- netmotion

- ogg
- openvpn
- quicktime
- rdt
- scydo
- spotify
- tango
- tunnelvoice
- ultrabac
- usenet
- whatsapp

CLI (Exec Mode)

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

show active-charging sessions summary

This command displays statistics for specific active charging service sessions. The output of this command includes the following new fields:

- Current ANTSP2P Sessions
- Current IMO Sessions
- Current MYPEOPLE Sessions
- Current NETMOTION Sessions
- Current OGG Sessions
- Current OPENVPN Sessions
- Current QUICKTIME Sessions
- Current RDT Sessions
- Current SCYDO Sessions
- Current SPOTIFY Sessions
- Current TANGO Sessions
- Current TUNNELVOICE Sessions
- Current ULTRABAC Sessions
- Current USENET Sessions
- Current WHATSAPP Sessions

CLI (Exec Mode)

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

show active-charging sessions summary type p2p

This command displays summary information for P2P active charging service sessions. The output of this command includes the following new fields:

- Current ANTSP2P Sessions
- Current IMO Sessions
- Current MYPEOPLE Sessions
- Current NETMOTION Sessions
- Current OGG Sessions
- Current OPENVPN Sessions
- Current QUICKTIME Sessions
- Current RDT Sessions
- Current SCYDO Sessions
- Current SPOTIFY Sessions
- Current TANGO Sessions
- Current TUNNELVOICE Sessions
- Current ULTRABAC Sessions
- Current USENET Sessions
- Current WHATSAPP Sessions

CLI (Exec Mode)

show active-charging sessions [full [wide] | summary | display-dynamic-charging-rules | dynamic-charging] { [all] | [*filter_keyword*] + } [| { grep *grep_options* | more }]

Content Filtering Commands - Modified in Release 12.0

The following commands have been modified in Release 12.0.

None for this release.

ECS Commands - Modified in Release 12.0

The following commands have been modified in Release 12.0.

clear active-charging tcp-proxy statistics

This command clears TCP Proxy related statistics. The **socket-migration** keyword was added to this command. This enables to clear TCP Proxy Socket Migration related statistics.

CLI (Exec Mode)

clear active-charging tcp-proxy statistics [all | ip-layer | rulebase *rulebase_name* | socket-migration | tcp-layer]

show active-charging flows full

This command displays active-charging flow information. The output of this command now includes the following TCP Proxy Socket Migration related fields:

- Socket Migration Details:
  - State
  - Highest ACK Frm Server
  - Highest Seq Frm Server
  - Highest ACK Frm MS
  - Highest Seq Frm MS
  - Seq Frm MS at Mig
  - ACK Frm MS at Mig
  - Seq Frm Server at Mig
  - ACK Frm Server at Mig
  - Data To Be Delivered To MS
  - Data To Be Delivered To Server
  - Highest Seq Frm MS
  - Timestamps Enabled
  - SACK Enabled
  - Wscale From MS
  - Wscale From Server

CLI (Exec Mode)

show active-charging flows full

show active-charging tcp-proxy statistics

This command displays TCP Proxy related statistics. The **socket-migration** keyword was added to this command. This enables to view TCP Proxy statistics for socket migration.

CLI (Exec Mode)

show active-charging tcp-proxy statistics [all | ip-layer | rulebase *rulebase_name* **| socket-migration | tcp-layer] [verbose] [| { grep** *grep_options* **| more }]**

ECS Commands - Modified in Release 12.2

The following commands have been modified in Release 12.2.

show cdr statistics

This command displays EDR and UDR file statistics. The output of this command now includes the following fields to count the number of billing records accumulated on the hard disk to transfer to L-ESS:

- Num of file Pend transfer
- Num of file Queued transfer

CLI (Exec Mode)

show cdr statistics

show active-charging dns-learnt-ip-addresses

This command displays the DNS learnt IP address statistics for the DNS Snooping feature. The output of this command now includes the following fields to display the summary of dynamic learnt IPv4 and IPv6 address:

- Total learnt ipv4 entries
- Total learnt ipv6 entries

CLI (Exec Mode)

show active-charging dns-learnt-ip-addresses statistics { sessmgr { all | instance *sessmgr_instance_number* **} [verbose] | summary } [| { grep** *grep_options* **| more }]**

show active-charging service all

This command displays detailed ACS service configuration information. The output of this command includes the following new counter:

Selection of Charging-rule-base: If multiple Charging-Rule-Base-Name AVP are received from the PCRF, indicates which rulebase is selected and applied to the call, the first or the last rulebase.

For more information, in the *Configuration Management* chapter see the **policy-control charging-rule-base-name** CLI command.

CLI (Exec Mode)

show active-charging service { all | name *acs_service_name* **} [| { grep** *grep_options* **| more }]**

Firewall Commands - Modified in Release 12.0

The following commands have been modified in Release 12.0.

clear active-charging firewall statistics

This command clears Active Charging Firewall statistics. The following keywords were added to this command:

- **icmpv6**
- **ipv6**

CLI (Exec Mode)

clear active-charging firewall statistics [callid *call_id* **| domain-name** *domain_name* **| nat-realm** *nat_realm* **| protocol { icmp | icmpv6 | ip | ipv6 | other | tcp | udp } | username** *user_name* **] [acsmgr instance** *instance_id* **] [| { grep** *grep_options* **| more }]**

clear subscribers

This command disconnects subscribers based on specified criteria.The following keywords were added to this command:

- **ipv4**
- **ipv6**

CLI (Exec Mode)

clear subscribers [*keywords* **] [verbose] [-noconfirm]**

show active-charging firewall statistics

This command displays Active Charging Firewall statistics. The following keywords were added to this command:

- **icmpv6**
- **ipv6**

CLI (Exec Mode)

show active-charging firewall statistics [callid *call_id* **| domain-name** *domain_name* **| nat-realm** *nat_realm* **| protocol { icmp | icmpv6 | ip | ipv6 | other | tcp | udp } | username** *user_name* **] [acsmgr instance** *instance_id* **] [verbose] [| { grep** *grep_options* **| more }]**

show active-charging firewall statistics verbose

This command displays Active Charging Stateful Firewall statistics. The output of this command includes the following new ICMPv6 and IPv6 statistics:

- ICMPv6 Stats:
  - Invalid ICMPv6 Response
  - ICMPv6 Reply Error
  - Invalid ICMPv6 Type Packet
  - ICMPv6 Error Message Replay Attacks
  - ICMPv6 Packets with Duplicate Sequence Number
  - Packets with Short ICMPv6 Header Length
  - Invalid ICMPv6 Packet Length
  - Packets Dropped on ICMPv6 Flood Attack
  - Ping Of Death Attacks
  - Packets Dropped due to ICMPv6 Checksum Errors
  - ICMPv6 Packets With Destination Unreachable Message
  - ICMPv6 Echo Packets Dropped due to ID Zero
- IPv6 Stats:
  - Land Attacks
  - Jolt Attacks
  - Teardrop Attacks
  - Invalid IP Option Length
  - IPv6 Source-router Attacks

- Packets with Short IPv6 Header Length
- Packets with Nested Fragmentation Header
- Packets with Unspecified IPv6 Address
- Packets with invalid Payload Length
- Packets with more than threshold Extension Headers
- Packets with invalid Hop By Hop Extension Header
- Packets with ICMPv4 in IPv6 Header
- Packets with invalid Destination Extension Header
- Downlink Dropped Bytes on IPv6 Reassembly Failure
- Uplink Dropped Bytes on IPv6 Reassembly Failure

CLI (Exec Mode)

show active-charging firewall statistics [callid *call_id* **| domain-name** *domain_name* **| nat-realm** *nat_realm* **| protocol { icmp | icmpv6 | ip | ipv6 | other | tcp | udp } | username** *user_name* **] [acsmgr instance** *instance_id* **] [verbose] [| { grep** *grep_options* **| more }]**

show active-charging firewall statistics callid <call_id> verbose

This command displays Active Charging Stateful Firewall statistics with Call ID. The output of this command includes the following new ICMPv6 statistics:

- ICMPv6 Stats:
  - Invalid ICMPv6 Response
  - ICMPv6 Reply Error
  - Invalid ICMPv6 Type Packet
  - ICMPv6 Error Message Replay Attacks
  - ICMPv6 Packets with Duplicate Sequence Number
  - Packets with Short ICMPv6 Header Length
  - Invalid ICMPv6 Packet Length
  - Packets Dropped on ICMPv6 Flood Attack
  - Ping Of Death Attacks
  - Packets Dropped due to ICMPv6 Checksum Errors
  - ICMPv6 Packets With Destination Unreachable Message
  - ICMPv6 Echo Packets Dropped due to ID Zero

CLI (Exec Mode)

show active-charging firewall statistics [callid *call_id* **| domain-name** *domain_name* **| nat-realm** *nat_realm* **| protocol { icmp | icmpv6 | ip | ipv6 | other | tcp | udp } | username** *user_name* **] [acsmgr instance** *instance_id* **] [verbose] [| { grep** *grep_options* **| more }]**

show active-charging firewall statistics domainname <domain_name> verbose

This command displays Active Charging Stateful Firewall statistics with Domain name. The output of this command includes the following new ICMPv6 statistics:

- ICMPv6 Stats:
  - Invalid ICMPv6 Response
  - ICMPv6 Reply Error
  - Invalid ICMPv6 Type Packet
  - ICMPv6 Error Message Replay Attacks
  - ICMPv6 Packets with Duplicate Sequence Number
  - Packets with Short ICMPv6 Header Length
  - Invalid ICMPv6 Packet Length
  - Packets Dropped on ICMPv6 Flood Attack
  - Ping Of Death Attacks
  - Packets Dropped due to ICMPv6 Checksum Errors
  - ICMPv6 Packets With Destination Unreachable Message
  - ICMPv6 Echo Packets Dropped due to ID Zero

CLI (Exec Mode)

show active-charging firewall statistics [callid *call_id* **| domain-name** *domain_name* **| nat-realm** *nat_realm* **| protocol { icmp | icmpv6 | ip | ipv6 | other | tcp | udp } | username** *user_name* **] [acsmgr instance** *instance_id* **] [verbose] [| { grep** *grep_options* **| more }]**

show active-charging firewall statistics username <user_name> verbose

This command displays Active Charging Stateful Firewall statistics with Username. The output of this command includes the following new ICMPv6 statistics:

- ICMPv6 Stats:
  - Invalid ICMPv6 Response
  - ICMPv6 Reply Error
  - Invalid ICMPv6 Type Packet
  - ICMPv6 Error Message Replay Attacks
  - ICMPv6 Packets with Duplicate Sequence Number
  - Packets with Short ICMPv6 Header Length
  - Invalid ICMPv6 Packet Length
  - Packets Dropped on ICMPv6 Flood Attack
  - Ping Of Death Attacks
  - Packets Dropped due to ICMPv6 Checksum Errors
  - ICMPv6 Packets With Destination Unreachable Message
  - ICMPv6 Echo Packets Dropped due to ID Zero

CLI (Exec Mode)

show active-charging firewall statistics [callid *call_id* **| domain-name** *domain_name* **| nat-realm** *nat_realm* **| protocol { icmp | icmpv6 | ip | ipv6 | other | tcp | udp } | username** *user_name* **] [acsmgr instance** *instance_id* **] [verbose] [| { grep** *grep_options* **| more }]**

show active-charging firewall statistics protocol icmpv6 verbose

This command displays Active Charging Stateful Firewall statistics for ICMPv6 protocol. The output of this command includes the following new ICMPv6 statistics:

- Firewall Statistics for Protocol: ICMPv6
- ICMPv6 Stats:
  - Invalid ICMPv6 Response
  - ICMPv6 Reply Error
  - Invalid ICMPv6 Type Packet
  - ICMPv6 Error Message Replay Attacks
  - ICMPv6 Packets with Duplicate Sequence Number
  - Packets with Short ICMPv6 Header Length
  - Invalid ICMPv6 Packet Length
  - Packets Dropped on ICMPv6 Flood Attack
  - Ping Of Death Attacks
  - Packets Dropped due to ICMPv6 Checksum Errors
  - ICMPv6 Packets With Destination Unreachable Message
  - ICMPv6 Echo Packets Dropped due to ID Zero
- Data Stats:
  - Total Packets Received
  - Total Bytes Received
  - Total Packets Sent
  - Total Bytes Sent
  - Total Packets Injected
  - Total Bytes Injected
  - Uplink Packets Dropped
  - Uplink Bytes Dropped
  - Downlink Packets Dropped
  - Downlink Bytes Dropped
  - Total Malformed Packets
  - Total DOS Attacks
  - Total Flows Processed by Firewall
  - Total NAT Flows Processed by Firewall

CLI (Exec Mode)

show active-charging firewall statistics [callid *call_id* **| domain-name** *domain_name* **| nat-realm** *nat_realm* **| protocol { icmp | icmpv6 | ip | ipv6 | other | tcp | udp } | username** *user_name* **] [acsmgr instance** *instance_id* **] [verbose] [| { grep** *grep_options* **| more }]**

show active-charging firewall statistics protocol ipv6 verbose

This command displays Active Charging Stateful Firewall statistics for IPv6 protocol. The output of this command includes the following new IPv6 statistics:

- Firewall Statistics for Protocol: IPv6
- IPv6 Stats:
  - Land Attacks
  - Jolt Attacks
  - Teardrop Attacks
  - Invalid IP Option Length
  - IPv6 Source-router Attacks
  - Packets with Short IPv6 Header Length
  - Packets with Nested Fragmentation Header
  - Packets with Unspecified IPv6 Address
  - Packets with invalid Payload Length
  - Packets with more than threshold Extension Headers
  - Packets with invalid Hop By Hop Extension Header
  - Packets with ICMPv4 in IPv6 Header
  - Packets with invalid Destination Extension Header
  - Downlink Dropped Bytes on IPv6 Reassembly Failure
  - Uplink Dropped Bytes on IPv6 Reassembly Failure
- Data Stats:
  - Total Packets Received
  - Total Bytes Received
  - Total Packets Sent
  - Total Bytes Sent
  - Total Packets Injected
  - Total Bytes Injected
  - Uplink Packets Dropped
  - Uplink Bytes Dropped
  - Downlink Packets Dropped
  - Downlink Bytes Dropped
  - Total Malformed Packets
  - Total DOS Attacks
  - Total Flows Processed by Firewall

- Total NAT Flows Processed by Firewall

CLI (Exec Mode)

show active-charging firewall statistics [callid *call_id* **| domain-name** *domain_name* **| nat-realm** *nat_realm* **| protocol { icmp | icmpv6 | ip | ipv6 | other | tcp | udp } | username** *user_name* **] [acsmgr instance** *instance_id* **] [verbose] [| { grep** *grep_options* **| more }]**

show active-charging fw-and-nat policy name

This command displays Firewall-and-NAT Policy information. The output of this command includes the following new fields:

- IPv6 Extension Headers Limit
- IPv6 Hop By Hop Options
- Hop By Hop Router Alert Option
- Hop By Hop Jumbo Payload Option
- Invalid Hop By Hop Options
- Unknown Hop By Hop Options
- IPv6 Destination Options
- Invalid Destination Options
- Unknown Destination Options
- IPv6 Nested Fragmentation

CLI (Exec Mode)

show active-charging fw-and-nat policy { { { all | name *fw_nat_policy_name* **} [service name** *acs_service_name* **] } | { statistics { all | name** *fw_nat_policy_name* **} } } [| { grep** *grep_options* **| more }]**

show active-charging fw-and-nat policy name

This command displays Firewall-and-NAT Policy information. The output of this command includes the following new fields:

- Firewall Status IPv4
- Firewall Status IPv6

CLI (Exec Mode)

show active-charging fw-and-nat policy { { { all | name *fw_nat_policy_name* **} [service name** *acs_service_name* **] } | { statistics { all | name** *fw_nat_policy_name* **} } } [| { grep** *grep_options* **| more }]**

show active-charging sessions

This command displays statistics for ACS sessions. The following keywords were added to this command:

- **ipv4**
- **ipv6**

CLI (Exec Mode)

show active-charging sessions [full [wide] | summary | display-dynamic-charging-rules | dynamic-charging] { [all] | [*filter_keyword*] + } [| { grep *grep_options* | more }]

show active-charging subsystem all

This command displays service and configuration counters for the active charging service. The output of this command includes the following new fields:

- Firewall IPv4
- Firewall IPv6

CLI (Exec Mode)

show active-charging subsystem { all | facility acsmgr { all | instance *instance_value* } [rulebase name *rulebase_name*] | sip } [| { grep *grep_options* | more }]

show subscribers

This command displays all available subscriber information. The following keywords were added to this command:

- **ipv4**
- **ipv6**

CLI (Exec Mode)

show subscribers [*command_keyword*] [*filter_keywords*] [| { grep *grep_options* | more }]

show subscribers full

This command displays all available subscriber information. The output of this command includes the following new fields:

- Firewall-and-Nat Policy
- Firewall Policy IPv4
- Firewall Policy IPv6

CLI (Exec Mode)

show subscribers [*command_keyword*] [*filter_keywords*] [| { grep *grep_options* | more }]

GGSN Commands - Modified in Release 12.0

The following commands have been modified in Release 12.0.

show dhcp-service

This command displays the service and configuration counters for a DHCP service. The output of this command includes following new field:

- DHCP chaddr validation

CLI (Exec Mode)

show dhcp-service name [*service_name* **]**

GGSN Commands - Modified in Release 12.2

show apn name

This command displays the service and configuration statistics for an APN. The output of this command now includes following new field:

- radius returned-username

Under the APN configuration, this option is to either use the username sent by RADIUS in Access-Accept or send the constructed username itself in the RADIUS Acct messages.

CLI (Exec Mode)

show apn name [*apn_name* **]**

show gtpu-service

This command displays configuration information for GPRS Tunneling Protocol user plane (GTP-U) services. The output of this command now includes following new field:

- Sequence Number

HA Commands - Modified in Release 12.0

The following commands have been modified in Release 12.0.

None for this release

HA Commands - Modified in Release 12.2

The following commands have been modified in Release 12.0.

None for this release.

HSGW Commands - Modified in Release 12.0

The following HSGW commands have been modified in Release 12.0.

show apn name

This command displays the service and configuration statistics for an APN. The output of this command now includes the following new field:

- Accounting Policy Name

Under the APN configuration, this option is used to associate an accounting policy.

CLI (Exec Mode)

show apn name [*apn_name* **]**

clear hsgw-service

The keyword **all** has been removed from this command.

CLI (Exec Mode)

clear hsgw-service statistics [name *service_name* **] [| { grep** *grep_options* **| more }]**

show hsgw-service

The keywords **statistics** and **pcf-status** have been added to this command.

CLI (Exec Mode)

show hsgw-service { all | name *service_name* **| statistics { all | name** *service _name* **} } [pcf-status [address** *IPv4_address* **| filter { all | icmp-monitored | no-calls | summary | up }] [| { grep** *grep_options* **| more }]**

show mag-service

The keyword **ip-address** has been added to this command.

CLI (Exec Mode)

show mag-service { all | name *service_name* **| session [all | callid** *id* **| counters | full | ip-address** *home_ip_address* **| msid** *id* **| summary | username** *name* **] | statistics [name** *service_name* **] } [| { grep** *grep_options* **| more }]**

HSGW Commands - Modified in Release 12.2

The following HSGW commands have been modified in Release 12.2.

show gtpu-service

This command displays configuration information for GPRS Tunneling Protocol user plane (GTP-U) services. The output of this command now includes following new field:

- Sequence Number

show mag-service

This command displays statistic and counter information for Mobile Access Gateway (MAG) services. The output of this command now includes the following new field:

- IPv6 Traffic

This field displays if IPv6 Traffic is Disabled.

CLI (Exec Mode)

show mag-service session full

show subscribers

This command displays information for subscriber sessions. The output of this command now includes the following new field:

- IPv6 Traffic

This field displays if IPv6 Traffic is Disabled.

CLI (Exec Mode)

`show subscribers full (HSGW call)`

IPCF Commands - Modified in Release 12.1

This section provides information on modified IPCF commands in Release 12.1.

IPCF is new product for this release.

Mobility Management Entity Commands - Modified in Release 12.0

The following Mobility Management Entity (MME) commands are modified in Release 12.0.

monitor subscriber

The following output fields now show “n/a” (Not applicable) instead of being blank when issuing this command.

- IMEI
- Username

Exec Mode

monitor subscriber

show mme-service

The following commands have been enhanced to include the **ipsec** keyword option.

CLI (Exec Mode)

show mme-service enodeb-association [summary | full] [all | ipsec | mme-service-name *mme_svc_name* **| peer-address** *peer_ip_address* **| peer-id** *peer_identifier* **] [| { grep** *grep_options* **| more }]**

show mme-service session [summary | full | counters] [all | call-id *call_identifier* **| imei** *imei_id* **| imsi** *imsi_id* **| ipsec | mme-service** *service_name* **| msisdn** *number* **| pdn-address** *pdn_ip_address* **| s1-peer** *s1_peer_ip_address* **| s11- peer** *s11_peer_ip_address* **| ue-ecm-state { connected | idle }] [| { grep** *grep_options* **| more }**]

show mme-service session full

This command no longer includes the following fields showing authentication information about the session.

- Authentication Information
  - RAND: Random Number
  - XRES: Expected Response
  - K-ASM: Key-Authentication Security Model
  - AUTN: Authentication Token

CLI (Exec Mode)

show mme-service session full

show mme-service db record imsi

This command no longer displays the following fields showing authentication information.

- Security Context
  - Auth Status
  - Security Context Type
  - Ciphering Algo
  - Integrity Algo
  - NAS Count
  - NAS Overflow
  - NAS Integrity Key
  - NAS Ciphering Key

CLI (Exec Mode)

show mme-service db record imsi *<imsi>*

Mobility Management Entity Commands - Modified in Release 12.2

The following commands have been modified in Release 12.2.

show sgtpc statistics verbose

This command now includes the following new counter to show the number of GTPv0 messages dropped due to the user application not supporting GTP version 0.

```
GTPV0 msgs drpd due to no support in the usr app:                  0
```

CLI (Exec Mode)

show sgtpc statistics verbose

show mme-service session

This command now includes an option to filter the results based on Visitor Location Register (VLR) name.

CLI (Exec Mode)

show mme-service session full vlr-name *<vlr_name>*

show mme-service session vlr-name *<imsi>*

show egtpc sessions

The output of this command is now fully documented.

CLI (Exec Mode)

show egtpc sessions

show egtpc statistics verbose

This command has been enhanced to include 3GPP 29.274 and SRVCC statistics.

CLI (Exec Mode)

```
show egtpc statistics verbose
```

show mme-service statistics verbose

This command has been enhanced as follows:

- Add “Identity Response” under Total EMM Control Messages -Received
- Add “Deactivate Bearer Accepts” under Total ESM Control Messages - Sent
- Remove invalid EMM counters: Detach Request 0 IMSI Detach and TAU Reject - ESM Failure
- Remove invalid ESM counter: PDN Disconnect reject - Rejected By PGW/SGW.

CLI (Exec Mode)

```
show mme-service statistics verbose
```

NAT Commands - Modified in Release 12.0

The following commands have been modified in Release 12.0.

show active-charging sessions full

This command displays statistics for ACS sessions. The output of this command includes the following new field:

- Current H323 Flows

CLI (Exec Mode)

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

show active-charging sessions full all

This command displays statistics for ACS sessions. The output of this command includes the following new field:

- Current H323 Flows

CLI (Exec Mode)

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

show active-charging subsystem all

This command displays service and configuration counters for the active charging service. The output of this command includes the following new fields:

- Total H323 Flows
- Current H323 Flows

CLI (Exec Mode)

show active-charging subsystem { all | facility acsmgr { all | instance *instance_value* **} [rulebase name** *rulebase_name* **] | sip } [| { grep** *grep_options* **| more }]**

NAT Commands - Modified in Release 12.2

The following commands have been modified in Release 12.2.

show active-charging firewall statistics verbose

This command displays Active Charging Stateful Firewall statistics. The output of this command includes the following new fields:

- Packets dropped due to NAT Translation failed on unsupported ICMP code
- Packets dropped due to NAT Translation failed on invalid Param Problem
- Packets dropped due to IPv6 routing header with non-zero segments left
- Packets dropped due to Unsupported Embedded IPv4 Address
- Packets dropped due to Destination IPv6 Prefix Mismatch
- Total Packets (NAT64 Translation)
- Total Bytes Reduced (NAT64 Translation)
- Total NAT44 Flows Processed by Firewall
- Total NAT64 Flows Processed by Firewall
- Total Bypass-NAT Flows Processed by Firewall
- Total Bypass-NAT IPv4 Flows Processed by Firewall
- Total Bypass-NAT IPv6 Flows Processed by Firewall

CLI (Exec Mode)

show active-charging firewall statistics [callid *call_id* **| domain-name** *domain_name* **| nat-realm** *nat_realm* **| protocol { icmp | icmpv6 | ip | ipv6 | other | tcp | udp } | username** *user_name* **] [acsmgr instance** *instance_id* **] [verbose] [| { grep** *grep_options* **| more }]**

show active-charging fw-and-nat policy name

This command displays Firewall-and-NAT Policy information. The output of this command includes the following new fields:

- NAT Status NAT44
- NAT Status NAT64
- ICSR Flow-recovery Status
  - Non-ALG
  - SIP-ALG
  - H323-ALG

CLI (Exec Mode)

show active-charging fw-and-nat policy { { { all | name *fw_nat_policy name* **} [service name** *acs_service_name* **] } | { statistics { all | name** *fw_nat_policy_name* **} } } [| { grep** *grep_options* **| more }]**

show active-charging nat statistics

This command displays NAT realm statistics. The output of this command includes the following new fields:

- NAT44 flows denied IP
- NAT44 flows denied port
- NAT64 flows denied IP
- NAT64 flows denied port
- NAT44 bytes Transferred
- NAT44 flows processed
- NAT64 bytes Transferred
- NAT64 flows processed

CLI (Exec Mode)

show active-charging nat statistics [nat-realm *nat_realm* **[summary]] [| { grep** *grep_options* **| more }]**

show active-charging sessions full

This command displays statistics for ACS sessions. The output of this command includes the following new fields:

- NAT Policy NAT44
- NAT Policy NAT64

CLI (Exec Mode)

show active-charging sessions [full [wide] | summary | display-dynamic-charging-rules | dynamic-charging] { [all] | [*filter_keyword* **] + } [| { grep** *grep_options* **| more }]**

show active-charging sessions full all

This command displays statistics for ACS sessions. The output of this command includes the following new fields:

- NAT Policy NAT44
- NAT Policy NAT64

CLI (Exec Mode)

show active-charging sessions [full [wide] | summary | display-dynamic-charging-rules | dynamic-charging] { [all] | [*filter_keyword* **] + } [| { grep** *grep_options* **| more }]**

show active-charging sessions nat

This command displays statistics for ACS sessions. The following keywords are added to this command to display active-charging sessions for which NAT44/NAT64 processing is required:

- ipv6
- ipv6

CLI (Exec Mode)

show active-charging sessions nat { not-required | required [nat-realm *nat_realm* **] } [ipv4 | ipv6]**

show active-charging subsystem all

This command displays service and configuration counters for the active charging service. The output of this command includes the following new fields:

- NAT44 Enabled
- NAT64 Enabled

CLI (Exec Mode)

show active-charging subsystem { all | facility acsmgr { all | instance *instance_value* **} [rulebase name** *rulebase_name* **] | sip } [| { grep** *grep_options* **| more }]**

show configuration

Displays current configuration information for the card, context, port, or target configuration file as specified. The output of this command includes the following new field for non default configuration:

- nat icsr-flow-recovery

CLI (Exec Mode)

show configuration [card *card_name* **| context** *context_name* **[radius** *group* **[all | name** *group* **]] | port** *slot/port* **| srp] [showsecrets] [url** *url* **] [verbose] [| { grep** *grep_options* **| more }]**

show configuration verbose

Displays current configuration information for the card, context, port, or target configuration file as specified. The output of this command includes the following new field for default configuration:

- no nat icsr-flow-recovery

CLI (Exec Mode)

show configuration [card *card_name* **| context** *context_name* **[radius** *group* **[all | name** *group* **]] | port** *slot/port* **| srp] [showsecrets] [url** *url* **] [verbose] [| { grep** *grep_options* **| more }]**

show subscribers nat

This command displays all available subscriber information. The following keywords are added to this command to display subscribers for whom NAT44/NAT64 processing is required:

- ipv6
- ipv6

CLI (Exec Mode)

show subscribers nat { not-required | required [nat-ip *nat_ip_address* **|** **nat-realm** *nat_realm* **] } [ipv4 | ipv6]**

show subscribers full

This command displays all available subscriber information. The output of this command includes the following new fields:

- NAT Policy NAT44
- NAT Policy NAT64

CLI (Exec Mode)

show subscribers [*command_keyword* **] [** *filter_keywords* **] [| { grep** *grep_options* **| more }]**

Packet Data Network Gateway Commands - Modified in Release 12.0

The following P-GW commands have been modified in Release 12.0.

clear apn statistics

The keyword **smgr-instance** has been added to this command.

CLI (Exec Mode)

clear apn statistics [name *apn_name* **| smgr-instance** *instance* **] [| { grep** *grep_options* **| more }]**

clear pgw-service

The keyword **all** has been removed from this command.

CLI (Exec Mode)

clear pgw-service statistics [name *service_name* **] [| { grep** *grep_options* **| more }]**

show apn name

This command displays the service and configuration statistics for an APN. The output of this command now includes the following new field:

- Accounting Policy Name

Under the APN configuration, this option is used to associate an accounting policy.

CLI (Exec Mode)

show apn name [*apn_name* **]**

show crypto ipsec security-associations

The output of this command now includes the Diffie-Hellman group for each IPSec security association.

CLI (Exec Mode)

show crypto ipsec security-associations

show pgw-service

The keyword **verbose** has been added to this command.

CLI (Exec Mode)

show pgw-service { all | name *service_name* **| statistics { all | name** *service_name* **} [verbose] } [| { grep** *grep_options* **| more }]**

Packet Data Network Gateway Commands - Modified in Release 12.2

The following P-GW commands have been modified in Release 12.2.

show active-charging credit-control

This command displays statistics for Diameter/RADIUS Prepaid Credit Control Service in the Active Charging Service (ACS). The output of this command now includes the following new row:

- Backpressured

This row specifies the number of sessions in backpressured state and the number of categories that are blacklisted.

CLI (Exec Mode)

show active-charging credit-control sessions-states

show active-charging sessions

This command displays statistics for Active Charging Service (ACS) sessions. The output of this command now includes the following new field:

- Backpressured

This value shows how many times the category was subsequently moving into backpressured state (unable to send message due to message queue being full) while sending a CCR-U out. Maximum value is 15.

If this field is not displayed, the category is currently not in backpressured state.

CLI (Exec Mode)

show active-charging sessions full

show apn name

This command displays the service and configuration statistics for an APN. The output of this command now includes the following new field:

- radius returned-username

Under the APN configuration, this option is to either use the username sent by RADIUS in Access-Accept or send the constructed username itself in the RADIUS Acct messages.

CLI (Exec Mode)

show apn name [*apn_name* **]**

show gtpu-service

This command displays configuration information for GPRS Tunneling Protocol user plane (GTP-U) services. The output of this command now includes following new field:

- Sequence Number

show lma-service

This command displays statistic and counter information for Local Mobility Anchor (LMA) services. The output of this command now includes the following new field:

- IPv6 Traffic

This field displays if IPv6 Traffic is Disabled.

CLI (Exec Mode)

show lma-service session full

show subscribers

This command displays information for subscriber sessions. The output of this command now includes the following new field:

- IPv6 Traffic

This field displays if IPv6 Traffic is Disabled.

CLI (Exec Mode)

show subscribers full (P-GW call)

PDIF Commands - Modified in Release 12.0

The following commands have been modified in Release 12.0.

None for this release.

PDSN Commands - Modified in Release 12.0

The following commands have been modified in Release 12.0.

show active-charging sessions full all

The following keyword has been added to the command.

- full all

CLI (Config Mode)

`show active charging sessions full all`.

PDSN Commands - Modified in Release 12.2

The following commands have been modified in Release 12.0.

None for this release.

Serving Gateway Commands - Modified in Release 12.2

The following commands have been modified in Release 12.2.

show egtp statistics verbose

The output of the **`show egtpc statistics verbose`** command now includes detailed rejection statistics for the following call request/response/notification denials [3GPP Release 9, 29.274]:

- Reject Statistics
- Modify Bearer Request Denied
- Delete Bearer Request Denied
- Delete Session Request Denied
- Downlink Data Notification Denied
- Release Access Bearers Denied
- Create Bearer Denied
- Update Bearer Denied
- Delete Bearer Command Denied
- Modify Bearer Command Denied
- Bearer Resource Command Denied
- Create Indirect Data Forwarding Tunnel Request Denied
- Delete Indirect Data Forwarding Tunnel Request Denied
- Change Notification Request Denied
- Context Request Denied
- Context Response Denied
- Identification Request Denied
- Forward Relocation Request Denied
- Forward Access Context Notification Denied
- Forward Relocation Complete Notification Denied
- Relocation Cancel Request Denied

- Suspend Notification Denied
- Resume Notification Denied

CLI (Exec Mode)

show egtp statististics verbose

show gtpu-service

This command displays configuration information for GPRS Tunneling Protocol user plane (GTP-U) services. The output of this command now includes following new field:

- Sequence Number

show sgw-service

The output of the **show sgw-service** command now displays the currently configured Accounting Mode.

CLI (Exec Mode)

show sgw-service [all | name *sgw_srv_name* **]**

Session Control Manager Commands - Modified in Release 12.0

The following SCM commands have been modified in Release 12.0.

show cscf tcp

The keywords **msrp** and **sip** have been added to this command.

CLI (Exec Mode)

show cscf tcp connections service *service_name* **[facility { cscfmgr | sessmgr }] [full] [msrp] [remote-ip** *ip_address* **] [remote-port** *port_number* **] [sip] [| { grep** *grep_options* **| more }]**

Session Control Manager Commands - Modified in Release 12.2

The following SCM commands have been modified in Release 12.2.

clear crypto statistics

This command can now clear statistics for SRTP (Secure Real-time Transport Protocol).

CLI (Exec Mode)

clear crypto { isakmp [tag *map_name* **| peer** *peer_ip* **] | security-association { counters tag** *map_name* **[tx | rx] | tag** *map_name* **| peer** *peer_ip* **} | statistics { ikev2 | ipsec-3gpp-cscf | srtp } [service-ip-address** *ip_address* **| service-name** *service_name* **] }**

show crypto statistics

This command can now display SRTP (Secure Real-time Transport Protocol) statistics.

CLI (Exec Mode)

show crypto statistics ikev1 | ikev2 [service-ip-address *ip_address* **] [service-name** *service_name* **] | ipsec-3gpp-cscf [service-ip-address** *ip_address* **] [service-name** *service_name* **] | srtp [service-ip-address** *ip_address* **] [service-name** *service_name* **]**

show cscf service

This command displays configuration and/or statistic information for Call Session Control Function (CSCF) services on this system. The output of this command includes the following new fields to show additional statistics pertaining to AAR sent for INV, 18X and 2XX separately:

- DPECA Message Stats:
- Messages Sent
  - AAR-Invite
  - AAR-18X
  - AAR-2XX
- DPECA Message Stats:
- Messages Received
  - AAA-INVITE
  - AAR-18X
  - AAR-2XX

CLI (Exec Mode)

show cscf service diameter policy-control statistics service-name <*service_name***>**

show subscribers cscf-only

This command displays information for Call Session Control Function (CSCF) subscribers only. The output of this command now includes the field Private User ID.

CLI (Exec Mode)

show subscribers cscf-only full

EXAMPLE(S)

```
[local]asr5000# show subscribers cscf-only full
AoR: userA@192.208.2.11:5060            callid: 00004e21
  User-Agent: LGT-client/VT1.5 + MIM 1.0 SPH-W8350
  Private User ID: userAP@192.208.2.11
  I-Path: n/a
```

show subscribers summary

This command displays information for subscriber sessions. The output of this command now includes the following new fields:

- cscf-sip-v4

- cscf-sip-v6
- cscf-access-wifi
- cscf-access-evdo
- cscf-access-wcdma
- cscf-access-ehrpd
- cscf-ue-ims
- cscf-ue-nonims
- cscf-sip-pcscf
- cscf-sip-scscf
- cscf-sip-rfc3261
- cscf-access-wired
- cscf-access-1xcdma
- cscf-access-lte
- cscf-access-undetermined
- cscf-security-ipsec
- cscf-security-tls

These fields provide the IPv4/v6 subscriber count per PSC

Sample **`show subscribers summary`** output format:

Before:

```
cscf-sip:                       8
```

After:

```
cscf-sip:                       8            cscf-sip-pcscf:                4
cscf-sip-v4:                    8            cscf-sip-scscf:                4
cscf-sip-v6:                    0            cscf-sip-rfc3261:              0
cscf-access-wifi:               2            cscf-access-wired:             6
cscf-access-evdo:               0            cscf-access-1xcdma:            0
cscf-access-wcdma:              0            cscf-access-lte:               0
cscf-access-ehrpd:              0            cscf-access-undetermined:      0
cscf-ue-ims:                    8            cscf-security-ipsec:           0
cscf-ue-nonims:                 0            cscf-security-tls:             0
```

CLI (Exec Mode)

`show subscribers summary`

show subscribers summary cscf-service

This command displays information for cscf subscriber sessions. The output of this command now includes the following new fields:

- No of IPv4 subscribers : 1
- No of IPv6 subscribers : 0
- No of PCSCF subscribers : 1
- No of SCSCF subscribers : 0
- No of RFC3261 subscribers :0
- No of WiFi subscribers : 0
- No of Wired subscribers : 1
- No of EvDO subscribers : 0
- No of WCDMA subscribers : 0
- No of 1xCDMA subscribers : 0
- No of LTE subscribers : 0
- No of EHRPD subscribers : 0
- No of undetermined access subscribers : 0
- No of IMS subscribers : 1
- No of non-IMS subscribers: 0
- No of IPSec subscribers : 0
- No of TLS subscribers : 0
- No of Domain cisco1.com subscribers : 1

These fields provide the IPv4/v6 subscriber count per PSC

Sample **`show subscribers summary cscf-service <`***`cscfservice`***`>`** output format:

Before:

```
Registered subscribers   : 4

Unregistered subscribers : 0

Access service collapsed : 0

No. of CSCF sessions     : 0

Mobile originated calls  : 0

Mobile terminated calls  : 0

Network to network calls : 0
```

After:

```
Registered subscribers   : 4

Unregistered subscribers : 0

Access service collapsed : 0
```

```
No. of CSCF sessions     : 0
Mobile originated calls  : 0
Mobile terminated calls  : 0
Network to network calls : 0
No of IPv4 subscribers   : 4
No of IPv6 subscribers   : 0
No of PCSCF subscribers  : 4
No of SCSCF subscribers  : 0
No of RFC3261 subscribers :0
No of WiFi subscribers   : 1
No of Wired subscribers  : 3
No of EvDO subscribers   : 0
No of WCDMA subscribers  : 0
No of 1xCDMA subscribers : 0
No of LTE subscribers    : 0
No of EHRPD subscribers  : 0
No of undetermined access subscribers : 0
No of IMS subscribers    : 4
No of non-IMS subscribers: 0
No of IPSec subscribers  : 0
No of TLS subscribers    : 0
No of Domain 192.168.145.150 subscribers : 2
No of Domain starent.com subscribers : 2
```

CLI (Exec Mode)

show subscribers summary cscf-service *cscf_service*

SGSN Commands - Modified in Release 12.0

The following commands have been modified in Release 12.0 - unless otherwise indicated, the listed fields have been added to the output displays:

show apn-profile full name <profile_name>

- APN Name
- Quality of Service Capping
- Prefer Type
- Traffic Class

- SDU delivery order
- Delivery Of Erroneous Sdus
- Convert Max Bit Rate Uplink From
- Convert Max Bit Rate Downlink From
- SDU Max Size
- DNS Extension with LAC-RAC

show apn-remap-table full name

- Fallback APN to use when Default APN not present in subscription

show bssgp statistics

- packets dropped due to clearing subscriber

show bssgp statistics verbose

- Attach Accept Message Statistics
- Attach Accept Message Statistics received in bssgp
- Attach Accept Message Statistics present in MS flow-control queue
- Attach Accept Message Statistics present in BVC flow-control queue
- Attach Accept Message Statistics dropped from MS flow-control queue
- Attach Accept Message Statistics dropped from BVC flow-control queue
- Attach Accept Message Statistics packets sent to NS layer
- Attach Accept Message Statistics dropped due to congestion in MS FLC

show bulkstats

A keyword has been added to the command to display the DLCI utilization variables.

CLI (Exec Mode)

```
show bulkstat variables dlci-util
```

show call-control-profile full all

- PTMSI-Signature-Realloc Attach Access-Type
- PTMSI-Signature-Realloc Attach Frequency value UMTS
- PTMSI-Signature-Realloc Attach Frequency value GPRS
- PTMSI-Signature-Realloc Interval Access-Type
- PTMSI-Signature-Realloc Interval value UMTS
- PTMSI-Signature-Realloc Interval value GPRS
- PTMSI-Signature-Realloc Frequency Access-Type
- PTMSI-Signature-Realloc Frequency value UMTS
- PTMSI-Signature-Realloc Frequency value GPRS
- PTMSI-Signature-Realloc RAU(Generic)Access-Type
- PTMSI-Signature-Realloc RAU(Generic) Frequency value UMTS
- PTMSI-Signature-Realloc RAU(Generic) Frequency value GPRS

- PTMSI-Signature-Realloc RAU Periodic Access-Type
- PTMSI-Signature-Realloc RAU Periodic Frequency value UMTS
- PTMSI-Signature-Realloc RAU Periodic Frequency value GPRS
- PTMSI-Signature-Realloc RAU RA Update Access-Type
- PTMSI-Signature-Realloc RAU RA Update Frequency value UMTS
- PTMSI-Signature-Realloc RAU RA Update Frequency value GPRS
- PTMSI-Signature-Realloc RAU Combined Update Access-Type
- PTMSI-Signature-Realloc RAU Combined Update Frequency value UMTS
- PTMSI-Signature-Realloc RAU Combined Update Frequency value GPRS
- PTMSI-Signature-Realloc RAU Imsi Combined Update Access-Type
- PTMSI-Signature-Realloc RAU Imsi Combined Update Frequency value UMTS
- PTMSI-Signature-Realloc RAU Imsi Combined Update Frequency value GPRS
- Authentication SMS
- Authentication SMS Access-Type
- Authentication SMS Frequency
- Authentication SMS (MO-SMS)
- Authentication SMS (MO-SMS) Access-Type
- Authentication SMS (MO-SMS) Frequency
- Authentication SMS (MT-SMS)
- Authentication SMS (MT-SMS) Access-Type
- Authentication SMS (MT-SMS) Frequency

show configuration

- gmm-message attach-with-tlli-in-use discard-message
- old-tlli invalidate tlli <*hex*>
- old-tlli invalidate tlli <*hex*>
- old-tlli hold-time <*seconds*>

show gmm-sm statistics verbose

- 2G-Failure due to Internal Error:
- IMEI black listed:
- APP Init Abort:
- Identity Send Failed:
- Page-Requests-Per-LA:
- Ret-Page-Requests-Per-LA:
- Page-Requests-Per-RA:
- Ret-Page-Requests-Per-RA:
- CAMEL Subscription Ignored:
- Modify-Request Abort:

- 3G-Modify-Request Abort:
- 2G-Modify-Request Abort:
- irat-att-dsd-rcvd-in-2g
- irat-att-cl-sub-in-2g
- pac-drop-att-rau-ongoing
- ActivateContextRequest
- Total-Actv-Request
- 3G-Actv-Request
- 2G-ActvRequest
- Primary-Actv-Request
- 3G-Primary-Actv-Request
- 2G-Primary-Actv-Request
- Secondary-Actv-Request
- 3G-Secondary-Actv-Request
- 2G-Secondary-Actv-Request
- Actv-Request-Nrpca
- Actv-Request-Mbms
- ActivateContextAccept
- Total-Actv-Accept
- 3G-Actv-Accept
- 2G-ActvAccept
- Primary-Actv-Accept
- 3G-Primary-Actv-Accept
- 2G-Primary-Actv-Accept
- Secondary-Actv-Accept
- 3G-Secondary-Actv-Accept
- 2G-Secondary-Actv-Accept
- Actv-Mbms-Accept
- 3G-Actv-Mbms-Accept
- ActivateContextReject
- Total-Actv-Reject
- 3G-Actv-Reject
- 2G-Actv-Reject
- Primary-Actv-Reject
- 3G-Primary-Actv-Reject
- 2G-Primary-Actv-Reject
- Secondary-Actv-Reject
- 3G-Secondary-Actv-Reject

- 2G-Secondary-Actv-Reject
- RequestPdpContextActivationReject
- Total-Request-Pdp-Ctxt-Reject
- 3G-Request-Pdp-Ctxt-Reject
- 2G-Request-Pdp-Ctxt-Reject
- GPRS-Attach Network Failure Cause
- Total 2G-external Triggers
- 2G-Data missing from HLR
- 2G-Throttling due to Congest
- 2G-Check IMEI timeout EIR
- 2G-Operator Policy Failure
- Comb-Attach Network Failure Cause
- Total 3G-Network Fail rejects
- Total 3G-external Triggers
- 3G-Data missing from HLR
- 3G-Throtling due to congest
- 3G-Check IMEI timeout EIR
- 3G-RNC Overload
- 3G-Operator Policy Failure
- 3G-Too many Ius same IMSI
- Total 3G-Internal Triggers
- 3G-Session mngr no resource

The following counters have been obsoleted and removed from the output display:

- Local Tlli
- IMSI Attach For SMID
- SMID SLIST Insert Failed
- CLP or SMID not found
- Incorrect State(Intra RAU)
- Incorrect State(Detached)

The following counters are new network-sharing counters for attach reject cause:

- Redirection Indication:
- PLMN not allowed:
- Location area not allowed
- Tot-Attach-Rej:
- Tot-Attach-Rej:
- Attach-Gprs:
- Attach-Gprs:

- Attach-Comb:
- Attach-Comb:
- Tot-Rau-Rej:
- Tot-Rau-Rej:
- Rau-Periodic:
- Rau-Periodic:
- Rau-Intra-SGSN:
- Rau-Intra-SGSN:
- Rau-Comb-Intra-SGSN:
- Rau-Comb-Intra-SGSN:
- Rau-Inter-SGSN:
- Rau-Inter-SGSN:
- Rau-Comb-Inter-SGSN:
- Rau-Comb-Inter-SGSN:
- Rau-Inter-Rat:
- Rau-Inter-Rat:
- Rau-Comb-Inter-Rat:
- Rau-Comb-Inter-Rat:
- Rau-Inter-Serv:
- Rau-Inter-Serv:
- Rau-Comb-Inter-Serv:
- Rau-Comb-Inter-Serv:
- Tot-Serv-Rej:
- Tot-Serv-Rej:
- Roaming not allowed in LA:
- No GPRS services in PLMN:
- Tot-Attach-Rej:
- Tot-Attach-Rej:
- Attach-Gprs:
- Attach-Gprs:
- Attach-Comb:
- Attach-Comb:
- Tot-Rau-Rej:
- Tot-Rau-Rej:
- Rau-Periodic:
- Rau-Periodic:
- Rau-Intra-SGSN:
- Rau-Intra-SGSN:

- Rau-Comb-Intra-SGSN:
- Rau-Comb-Intra-SGSN:
- Rau-Inter-SGSN:
- Rau-Inter-SGSN:
- Rau-Comb-Inter-SGSN:
- Rau-Comb-Inter-SGSN:
- Rau-Inter-Rat:
- Rau-Inter-Rat:
- Rau-Comb-Inter-Rat:
- Rau-Comb-Inter-Rat:
- Rau-Inter-Serv:
- Rau-Inter-Serv:
- Rau-Comb-Inter-Serv:
- Rau-Comb-Inter-Serv:
- Tot-Serv-Rej:
- Tot-Serv-Rej:
- CS/PS co-ord required:
- Unknown Reasons:
- Tot-Attach-Rej:
- Tot-Attach-Rej:
- Attach-Gprs:
- Attach-Gprs:
- Attach-Comb:
- Attach-Comb:
- Tot-Rau-Rej:
- Tot-Rau-Rej:
- Rau-Periodic:
- Rau-Periodic:
- Rau-Intra-SGSN:
- Rau-Intra-SGSN:
- Rau-Comb-Intra-SGSN:
- Rau-Comb-Intra-SGSN:
- Rau-Inter-SGSN:
- Rau-Inter-SGSN:
- Rau-Comb-Inter-SGSN:
- Rau-Comb-Inter-SGSN:
- Rau-Inter-Rat:
- Rau-Inter-Rat:

- Rau-Comb-Inter-Rat:
- Rau-Comb-Inter-Rat:
- Rau-Inter-Serv:
- Rau-Inter-Serv:
- Rau-Comb-Inter-Serv:
- Rau-Comb-Inter-Serv:
- Tot-Serv-Rej:
- Tot-Serv-Rej:
- Activate Context Reject Segregation:
- Total-3G-Actv-Reject:
- External Triggered:
- Internal Triggered:
- 3G-Primary-Actv-Reject:
- External Triggered:
- Internal Triggered:
- 3G-Secondary-Actv-Reject:
- External Triggered:
- Internal Triggered:
- Activate Primary PDP Context Insufficient Resource Cause Segregation:
- Total 3G-Insuff res triggers:
- Total 3G-Insuff res external triggs:
- 3G-Qos Negotiation Fail:
- 3G-Operator Policy Fail:
- 3G-GGSN Has No Resources:
- 3G-GGSN Changed PDP Type:
- 3G-GGSN PDP Addr Alloc Fail:
- 3G-RNC GTPU Path Failure:
- 3G-RNC RAB Establishment Fail:
- Total 3G-Insuff res internal triggs:
- 3G-SGSN Has No Memory:
- Activate Secondary PDP Context Insufficient Resource Cause Segregation:
- Total 3G-Insuff res triggers:
- Total 3G-Insuff res external triggs:
- 3G-Qos Negotiation Fail:
- 3G-Operator Policy Fail:
- 3G-Primary is GTPV0:
- 3G-GGSN Has No Resource:
- 3G-PDP Addr Type Mismatch:

- 3G-RNC GTPU Path Failure:
- 3G-RNC RAB Establishment Fail:
- 3G-Ongoing Bundle Deactivation:
- Total 3G-Insuff res internal triggs:
- 3G-SGSN Has No Memory:

The following new stats peg both ongoing procedure collisions and internal failures for 2G activation failures

- 2G-Actv Failure:
  - Internal Failure:
  - Ongoing Procedure:
- 2G-Primary-Actv-Failure:
  - Internal Failure:
  - Ongoing Procedure:
- 2G-Secondary-Actv-Failure:
  - Internal Failure:
  - Ongoing Procedure:
- 2G-Activation-Internal-Failure-Causes:
  - Resource Alloc Fail:
  - CPC Send Fail:

IMPORTANT

During some PDP activations both activation rejects and activation failures may be pegged if the SGSN is unable to proceed with request; e.g., SGSN will send out "Activation Reject" if it is unable to allocate memory to create PDP context for the subscriber and in this case both “Activation Reject” and “Activation Failure” will be pegged.

- 3G-PS-Page-Attempts

The behavior has changed for the following counters based on the configuration of the command “gmm-sm-statistics”:

- 2G-Network Failure
- Total-Attach-Reject
- 2G-Attach-Reject
- 3G-Network Failure
- 3G-Attach-Reject

When the configuration command “gmm-sm-statistics attach-rejects cause network-failure only-internal” (In SGSN Global Configuration Mode) is executed, this counter accounts only for the internal triggers that lead 2G/3G GPRS and Combined Attach Reject scenarios. If the command “no gmm-sm-statistics attach-rejects” is executed (This is the default behavior), this counter accounts for both the internal and external triggers that lead 2G/3G GPRS and Combined Attach Reject scenarios.

show gprsns statistics

- Number of ns-block dropped due to invalid nsvc
- Number of ns-block-ack dropped due to invalid nsvc
- Number of ns-status dropped due to invalid nsvc

show gprsns status

The new **nsvc-status-all** keyword has been added to display the status of all NSVC

CLI (Exec Mode)

```
show gprsns status nsvc-status-all
```

show gprs-service

The following field has been removed as it is not configurable:

- GMM LLC MAX Retries

show gprs-service all

The following fields have been added in a GMM Message Handler display:

- Procedure
- Condition
- Action

The following fields have been added to track use of random IOV-UI values in XID messages and to track the number of Attach failures due to the XID Response failure after the authentication procedure:

- GMM accept procedure : old tlli
- LLC IOVUI in xid-reset : send
- LLC IOVUI val in xid-reset: Random value
- LLC Reset VUR during intra RAU : Disabled
- LLC detect overflow : Disabled

show linecard

A keyword has been added to the command to display the DLCI utilization counters for a specific card.

CLI (Exec Mode)

```
show linecard dlci-utilization <card#>
```

show linecard dlci-utilization

The following utilization counters have been added to this new display output:

- Port
- Path
- E1T1
- TS
- DLCI
- NSE
- NSVC
- Average DLCI Utilization
  - Current Rx
  - Current Tx
  - 5 min Rx
  - 5 min Tx
  - 15 min Rx
  - 15 min Tx

show linkmgr all parser statistics

The following new counters have been added for the display output of the command:

- FWD Cont
- RCD Cont
- FWD Cont Error
- Free Dlg Count

New keyword, **`sgsn-empty-cr,`** has been added to display statistics supporting the handling of empty SCCP CRs.

CLI (Exec Mode)

```
show linkmgr { all | instance <> } parser statistics sgsn-empty-cr
```

The following new counters have been added for this new display output:

- SGSN Empty-Cr Statistics
- Empty-Cr sent to Imsimgr : 4
- Msg from Peer
- Released Rcvd :
- Rel Complete Rcvd :
- Inactivity Rcvd :
- Error Rcvd :
- DT1 Rcvd :
- DT1 DLR Modify :
- DT1 Decode attempt :
- Ranap Decode
- Init-UE Rcvd :

- Other Rcvd :
- Gmm Decode
- Gmm Rcvd :
- Attach Rcvd :
- Rau Rcvd :
- Detach Rcvd :
- Service Req Rcvd :
- Decoded DT1 msg
- Rau (Non-Local Old RAI):
- Rau (Local Old RAI) :
- Rau(LOR) diff Inst :
- Rau (LOR) Same Inst :
- Service/Detach Req :
- Serv/Detach diff Inst :
- Serv/Detach Same Inst :
- DT1 to be Fwd on Host cc :
- Msg to Donor Smgr
- Freezed Sent :
- Msg to Host Smgr
- CR Sent :
- Msg from Donor Smgr
- CC Rcvd :
- CREF Rcvd :
- Released Rcvd :
- Rel Complete Rcvd :
- Inactivity Rcvd :
- Error Rcvd :
- DT1 Rcvd :
- Others :
- Msg from Host Smgr
- CC Rcvd :
- CREF Rcvd :
- Released Rcvd :
- Rel Complete Rcvd :
- Inactivity Rcvd :
- Error Rcvd :
- DT1 Rcvd :
- Others :

- Local Purge :
- Failures
- CR Excess Len (>24) :
- Mem alloc fail Cb :
- Cb List insert fail :
- Duplicate Connection :
- DLR mdfy Buff Rem Fail :
- DLR mdfy Buff Add Fail:
- Lmgr UDatInd Fail :
- Lmgr Empty-cr Cb release reason
- Attach Request :
- Rau(Non local Old RAI):
- Rau (LOR)Same Inst :
- Serv/Detach Same Inst :
- Rel Complete from Peer :
- Rel Complete Local :
- Local Purge :
- CRef from Donor smgr :
- CRef from Host smgr :
- Guard timer Exp :
- Recovery :
- Others :

show linkmgr { all | instance <>} parser statistics memory

- SGSN-EMPCR entry

Enter the following modified CLI to dump empty-cr detail for a particular Session Manager associated with a specified LinkMgr:

```
show sgsn linkmgr instance <1-4> sgsn-empty-cr [ donor smgr-instance
<1-384> | host smgr-instance <1-384> ]
```

show llc statistics verbose

The following new field has been added to clarify Sessmgr WARN states:

- Known MS unexpected sapi

show session disconnect-reasons

The following SGSN-supported session disconnect reasons are new in this release:

- sgsn-ard-failure(436)
- sgsn-camel-release(437)

- sgsn-zone-code-failure(455)

The following session disconnect reasons are visible in this release but are in development for a future release:

- sgsn-egtpc-connection-failed(438)
- sgsn-egtpc-create-session-failed(439)
- sgsn-hss-detach(440)
- sgsn-hss-connection-failure(441)
- sgsn-pgw-detach(442)
- sgsn-s5-not-supported-for-apn(443)
- sgsn-no-rab-for-gbr-bearer(444)
- sgsn-sgw-selection-failure(445)
- sgsn-pgw-selection-failure(446)

show sgsn-fast-path statistics

- Total number of Bad Stats rcvd from NPU 1:

show sgsn-mode

- PDP Deactivation Rate per Session Manager
- Connected/Ready Mode Subscribers:
- Idle/Stand-By Mode Subscribers :

show sgsn-service

- Inform RNC before UE during QOS Modification

show sgtpc statistics verbose

- Note Ms Gprs Present Req Denied:
- Mandatory IE Incorrect
- Mandatory IE Missing
- Optional IE Incorrect
- Invalid Message Format
- GTPV0 msgs drpd due to no support in the usr app

show sgtp-service all

- GTP-C IP QOS DSCP value
- Gn Delay Monitoring
- Response wait time
- Delay responses to flag delay
- Normal responses to clear delay

show snmp trap statistics verbose

- SGSNGnMsgDelay
- SGSNGnMsgDelayClear

show ss7rd all sctp asp all status peer-server all peer-server-process all verbose

- Peer RWND
- Self RWND
- SSThresh
- Partial Bytes Acked
- Current RTO for this Path(in ms)
- Advertised RWND in received SACK

show ss7-routing-domain <ss7rd_id> mtp2 statistics linkset all link all

- Number of SIN packets transmitted
- Number of SIE packets transmitted
- Number of SIOS packets transmitted
- Number of SIPO packets transmitted
- Number of SIB packets transmitted
- Number of SIN packets received
- Number of SIE packets received
- Number of SIOS packets received
- Number of SIPO packets received
- Number of SIB packets received

show subs [grps-only | sgsn-only] full

- Number of Free Vectors:
- Number of Used Vectors:
- Number of In-Use Vectors:

SGSN Commands - Modified in Release 12.2

The following commands have been modified in Release 12.2

clear bssgp statistics

With new keywords, it is now possible to clear BSSGP statistics for specific BVCI or NSEI

CLI (Exec Mode)

```
clear bssgp statistics nse <nseid> [ bvc <bvci> ]
```

show gmm-sm statistics

New PLMN keyword set makes it possible to limit the display of GMM statistics for a specific PLMN:

CLI (Exec Mode)

```
show gmm-sm statistics [ gmm-only | plmn-id mcc <mcc> mnc <mnc> [
access-type { gprs | umts } ] | sm-only ] [ gprs-service <srvc_name> |
```

iups-service <*srvc_name*> | sgsn-service <*srvc_name*>] [verbose] [| { grep grep_options | more }]

show ip traffic

New **sctp** keyword obtains kernel SCTP traffic information for the specified card and CPU in a particular context.

CLI (Exec Mode)

show ip traffic sctp card <*slot_number*> cpu <*cpu_number*>

show linecard dlci-utilization

The following utilization counters have been added to this new display output:

- Port
- Path
- E1T1
- TS
- DLCI
- NSE
- NSVC
- Average DLCI Utilization
  - Current Rx
  - Current Tx
  - 5 min Rx
  - 5 min Tx
  - 15 min Rx
  - 15 min Tx

show session disconnect-reasons

The following session disconnect reasons is new in this release:

- **sgsn-rnc-no-dual-pdp-init-pdp-deact(458)**

show subscribers

The new **wide-format** keyword presents a wider screenful of information. This has been done to support more information in the IP field to support IPv4v6.

CLI (Exec Mode)

show subscribers sgsn-only wide-format

TPO Commands - Modified in Release 12.0

The following Traffic Performance Optimizer (TPO) have been modified in release 12.0.

show active-charging tpo profile statistics

This command displays TPO profile statistics. The output of this command includes the following new fields:

- Number of times TPO is disabled by P2P
- Number of times the TPO profile is selected

CLI (Exec Mode)

show active-charging tpo profile statistics [name *tpo_profile_name* **| all] [| { grep** *grep_options* **| more }]**

Obsolete Commands

This section identifies performance management commands obsoleted in Release 12.x.

Common Commands - Obsolete in Release 12.0

The following common commands are now obsolete in Release 12.0.

save logs facility

CLI (Exec Mode)

`save logs facility` *`facility`*

Application Detection and Control Commands - Obsolete in Release 12.0

The following commands are now obsolete in Release 12.0.

None for this release.

Content Filtering Commands - Obsolete in Release 12.0

The following commands are now obsolete in Release 12.0.

None for this release.

ECS Commands - Obsolete in Release 12.0

The following commands are now obsolete in Release 12.0.

None for this release.

Firewall Commands - Obsolete in Release 12.0

The following commands are now obsolete in Release 12.0.

None for this release.

GGSN Commands - Obsolete in Release 12.0

The following commands are now obsolete in Release 12.0.

None for this release.

HA Commands - Obsolete in Release 12.0

The following commands are now obsolete in Release 12.0.

None for this release.

IPCF Commands - Obsolete in Release 12.1

This section provides information on obsolete IPCF commands in Release 12.1.

IPCF is new product for this release.

Mobility Management Entity - Obsolete in Release 12.0

The following commands are now obsolete in Release 12.0.

show mme-policy

The **show mme-policy** command is no longer available in release 12.0 It has been replaced with the **show lte-policy** command.

CLI (Exec Mode)

show mme-policy { ho-restriction-list { name *name* **| subscriber-map { name** *name* **| summary } | tai-mgmt-db { name** *name* **| summary } } [| { grep** *grep_options* **| more }]**

NAT Commands - Obsolete in Release 12.0

The following commands are now obsolete in Release 12.0.

None for this release.

PDSN Commands - Obsolete in Release 12.0

The following commands are now obsolete in Release 12.0.

None for this release.

SGSN Commands - Obsolete in Release 12.0

The following commands are now obsolete in Release 12.0.

None for this release.

GTPP Storage Server Changes

The following commands are now obsolete in Release 12.0.

None for this release.

Web Element Manager Changes

There were no Web Element Manager changes in Release 12.0.

There were no Web Element Manager changes in Release 12.1.

There were no Web Element Manager changes in Release 12.2.

CHAPTER 6
SECURITY MANAGEMENT

This chapter identifies additions and changes made to security features in Release 12.0, 12.1, and 12.2.

Topics covered in this chapter are:

Security Configuration

This section identifies additions and changes made to the security features in Release 12.x.

Security Configuration Changes in Release 12.2

This section identifies additions and changes made to security features in Release 12.2.

New Commands

The following new commands were added for Release 12.2.

authorized-key

This command allows an operator to specify a username associated with SSHv2 DSA and/or RSA authorization keys. This user can access the sshd server to gain access to the ASR 5000.

CLI (SSH Configuration Mode)

[default] authorized-key username *user_name* **host** *host_name* **[type { v2-dsa | v2-rsa }]**

Modified Commands

None for this release.

Obsoleted Commands

None for this release.

Security Enhancements

This section identifies additions and changes made to the security features in Release 12.x.

Security Enhancements in Release 12.0

This section identifies additions and changes made to security features in Release 12.0.

None for this release

New Commands

None for this release.

Modified Commands

None for this release.

Obsoleted Commands

None for this release.

Security Enhancements in Release 12.1

This section identifies additions and changes made to the security features in Release 12.1.

None for this release.

New Commands

None for this release.

Modified Commands

None for this release.

Obsoleted Commands

None for this release.

Web Element Manager Security Configuration Changes in Release 12.0

This section identifies additions and changes made to security features in Release 12.0.

Secure Java Policy File Support

WEM now offers system administrators the option to use a secure java policy file to limit users' access to WEM servers' directory structure. Once the IP addresses of the WEM servers available are specified in the file, administrators can then set the allowed read/write/execute access permitted to users for each of those WEM servers.

For details on configuring and using the secure java policy file, refer to the *Web Element Manager Installation and Administration Guide*.

Apache Server Upgrade to Address Security Concerns

Certain security concerns due to issues with Apache Server 2.2.14 have been expressed.

Apache 2.2.14 is upgraded to Apache 2.2.21 for all new Solaris and RHEL WEM installations. Apache 2.2.21 is compiled with openSSL 0.9.8s version.

openSSL Upgrade to Address Security Concerns

Certain security concerns due to issues with openSSL have been expressed. Files are now recompiled with a later version of openSSL (0.9.8s).

Web Element Manager Security Configuration Changes in Release 12.2

This section identifies additions and changes made to security features in Release 12.2.

Adding, Deleting or Modifying a WEM User will Create Alarm

As part of an ongoing effort to increase WEM security, an alarm will now be generated whenever a WEM user is added, deleted or modified.

Default Map Drop-Down Box Added to Add User Dialog Box - General Tab

A Default Map combo box has been added which is populated with all the topology maps

that have been created by currently logged-in users.

The topology map is the default map view when a user opens WEM, so this combo box allows the Admin to select the appropriate map when creating a new user.

The selected map is created for the new user. When a newly created user logs into WEM for the first time, the selected default map would be displayed in the topology window. This means there is no need to create a default map again.

If the default map is changed in the Modify User screen, a new entry is added to the map table for that particular user.

WEM Path: Security Menu\User Administration\Dialog Boxes\Add User Dialog Box - General Tab

New User Profile Templates Support in Add User Dialog Box - General Tab

Instead of having to complete all required access fields when creating a new user in the Add User Dialog Box - General Tab, Administrators can create a dummy profile based on the fields required for the user type - Inspector, Operator, Config Admin or Security Admin - and that information can be saved as a profile. For example, *Inspector*. Next time a user is created needing Inspector privileges, the Admin can load the *Inspector* profile and the appropriate fields will be populated based on the dummy profile.

All fields can be saved in a dummy profile except the following:

Context Name

IMG List

User ID

Password

User Account Expiry

For example, if a new user is being created and requires Security Administrator privileges, first load the Security Administrator profile. Add the new User Name, Context Name, IMG List, User ID, User Account Expiry (if required)and Password. Enter a name for the profile in the Save Profile As field and click **Save** to create a user with Security Administrator profile and privileges.

WEM Path: Security Menu\User Administration\Dialog Boxes\Add User Dialog Box - General Tab