Cisco ASR 5000 Series Release 9.0 to Release 10.x Change Reference

Version 10.x

Generally Available 11-08-2010

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-22958-03

Cisco ASR 5000 Series Release 9.0 to Release 10.x Change Reference

TABLE OF CONTENTS

About This Guide

Chapter 1: New Feature Summary

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 guide identifies features and functionality added or modified between software releases 9.0 and 10.0. Topics covered in this chapter are:

Related Documents

Additional information on these items is located in the documents provided with the 10.0 and 10.2 release, see the table below.

Table 1-1 10.0 Release Documentation

Document	Part Number
Cisco ASR 5000 Series Product Overview Guide	OL-22938-02
Cisco ASR 5000 Series Packet Data Serving Node Administration Guide	OL-22939-02
Cisco ASR 5000 Series SNMP MIB Reference	OL-22942-02
Cisco ASR 5000 Series Gateway GPRS Support Node Administration Guide	OL-23696-01
Cisco ASR 5000 Series Command Line Interface Reference	OL-22948-03
Cisco ASR 5000 Series Enhanced Charging Services Administration Guide	OL-22951-01
Cisco ASR 5000 Series Session Control Manager Administration Guide	OL-22952-01
Cisco ASR 5000 Series Access Service Network Gateway Administration Guide	OL-23698-01
Cisco ASR 5000 Series AAA Interface Administration and Reference	OL-23000-02
Cisco ASR 5000 Series Release 9.0 to Release 10.0 Change Reference	OL-22958-03
Cisco ASR 5000 Series Content Filtering Services Administration Guide	OL-22959-01
Cisco ASR 5000 Series Peer-to-Peer Detection Administration Guide	OL-22960-01
Cisco ASR 5000 Series IP Services Gateway Administration Guide	OL-22961-01
Cisco ASR 5000 Series Packet Data Interworking Function Administration Guide	OL-22963-01
Cisco ASR 5000 Series Thresholding Configuration Guide	OL-22967-01
Cisco ASR 5000 Series System Administration Guide	OL-22970-02
Cisco ASR 5000 Series Home Agent Administration Guide	OL-22980-02
Cisco ASR 5000 Series Enhanced Feature Configuration Guide	OL-22983-01
Cisco ASR 5000 Series Packet Data Network Gateway Administration Guide	OL-22985-01
Cisco ASR 5000 Series Serving Gateway Administration Guide	OL-22986-01
Cisco ASR 5000 Series Mobility Management Entity Administration Guide	OL-22987-01
Cisco ASR 5000 Series Lawful Intercept Configuration Guide	OL-22988-01
Cisco ASR 5000 Series Statistics and Counters Reference	OL-22991-02
Cisco ASR 5000 Series Network Address Translation Administration Guide	OL-22992-01
Cisco ASR 5000 Series Mobility Unified Reporting System Installation and Administration Guide	OL-22993-01
Cisco ASR 5000 Series Aggregation Services Router Installation and Administration Guide	OL-22996-01
Cisco ASR 5000 Series Mobility Femto Gateway Administration Guide	OL-22997-01
Cisco ASR 5000 Series 3G Home NodeB Gateway Administration Guide	OL-22998-02
Cisco ASR 5000 Series Packet Data Gateway/Tunnel Termination Gateway Administration Guide	OL-22999-01
Cisco ASR 5000 Series External Storage Server Installation and Administration Guide	OL-22979-02

Common Features in Release 10.x

This section provides information on new features that are common to products in Release 10.0 and 10.2.

HNB-GW in UMTS Femto Network

The HNB-GW is new in Release 10.0.

With this release, Cisco Systems introduced Home-NodeB Gateway. The Home NodeB Gateway is the HNB network access concentrator used to connect the Home NodeBs (HNBs)/Femto Access Point (FAP) to access the UMTS network through HNB Access Network. It aggregates Home Node-B or Femto Access Points to a single network element and then integrates them into the Mobile Operators Voice, Data and Multimedia networks.

Benefits

The HNB-GW service is supported on Cisco's industry-leading ASR 5000 platforms, delivering unrivaled throughput, call transaction rates, and packet processing, along with significant memory resources.

In accordance with 3GPP standard, the HNB-GW provides following functions and procedures in UMTS core network:

- HNB Registration/De-registration Function
- UE Registration/De-registration Function for HNB
- Iuh User-plane Management Functions
- Iuh User plane Transport Bearer Handling
- Iu Link Management Functions

IMPORTANT

This is an indicative list of features supported in this release. Kindly contact your local Cisco representative for more information on supported features.

Description

The Home NodeB Gateway is the HNB access network gateway used to connect the Home NodeBs (HNBs) to access the existing wireless network. The HNB-GW concentrates connections from a large amount of femtocells (HNBs) using Iuh interface and terminates the connection to existing Core Networks (CS or PS) using the standard Iu (IuCS or IuPS) interface.

Femtocell is an important technology and service offering that enables new Home and Enterprise service capabilities for Mobile Operators and Converged Mobile Operators (xDSL/Cable/FFTH plus Wireless). The Femtocell network consists of a plug-n-play customer premise device generically called an Home NodeB (HNB) with limited range radio access in home or Enterprise. The HNB will auto-configure itself with the Operators network and the user can start making voice, data and multimedia calls.

For more information on this product, refer to *HNB Gateway Administration Guide*.

License Keys

Requires separate product license key.

Acceptance/Rejection of Messages with Different Origin Host - Behavioral Change

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

In earlier releases, a message received from a different host name was accepted only if the host was configured as a secondary host in the application configuration.

In this release, messages received with a different origin host are accepted if there is a route entry configured in the Diameter endpoint configuration.

To accept messages from host *host_x*, in the Diameter endpoint "**route-entry host** *host_x* **peer** *peer_y*" must be configured. The session will be bound to host *host_x* and all subsequent messages initiated from PCEF will have destination host as *host_x*.

Accounting Interim Request Messages - Behavioral Change

This Diameter-related behavioral change is applicable to all the LTE products using Rf Accounting interface.

In the earlier releases, if any accounting interim request message was pending at the Session Manager side, then any further interims were not sent for that session.

In the current release, accounting interim messages are allowed to be sent even if pending interim messages are present in the Session Manager for a particular session.

Bearer-Control-Mode AVP in CCA-I Messages

This Diameter-related behavioral change is applicable to all products that use R7/R8 Gx/Gxx interface, with the exception of HSGW/MIPV6HA/PDSN/HA releases to Verizon.

In the earlier releases, the Bearer-Control-Mode AVP was not considered as mandatory in CCA-I message sent by the PCRF. The sessions are established even when the Bearer-Control-Mode AVP is not included in the CCA-I.

In the current StarOS 10.0 release, if the PCEF does not receive this Bearer-Control-Mode AVP, the session will be terminated and CCR-T message will be sent to PCRF.

BCM Mode Validation against Network Request Supported AVP - Behavioral Change

This Diameter-related behavioral change is applicable to GGSN.

In earlier releases, the Bearer-Control-Mode received from PCRF was not validated in the GGSN.

In this release, if the GGSN broadcasts Network Request Support AVP as NOT supported, and PCRF sends BCM as UE_NW in CCA-I, the session will be terminated.

In case if GGSN broadcasts Network-Request-Support AVP as NOT supported, PCRF should authorize the BCM as UE_ONLY and not UE_NW.

BCM Value Negotiation for Different Service Types - Behavioral Change

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

In the previous releases, in case the PCRF did not send a Bearer-Control-Mode (BCM) in CCA-I, the PCEF terminated the session.

In the current release, if the BCM AVP is not received from PCRF, the IP-CAN session is not terminated. The value negotiated between UE/SGSN/GGSN is considered as the BCM.

The following values are considered for each of the service types.

- GGSN: The negotiated value between UE/SGSN/GGSN is considered.

  In the following scenarios UE_ONLY is chosen as the BCM:

  Scenario 1:

  - UE-> UE_ONLY
  - SGSN-> UE_ONLY
  - GGSN-> UE_ONLY
  - PCRF-> NO BCM

  Scenario 2:

  - UE-> UE_ONLY
  - SGSN-> UE_ONLY
  - GGSN-> Mixed
  - PCRF-> NO BCM
- GTP-PGW: BCM of UE_NW is considered.
- IPSG: BCM of UE_ONLY is considered.
- HSGW/SGW/PDIF/FA/PDSN/HA/MIPV6HA: BCM of NONE is considered.

Bidirectional Filters for Packet-Filter-Content AVP - Behavioral Change

This Diameter-related behavioral change is applicable to all products that use the R8 Gx interface.

In the earlier releases, the bidirectional filters were not checked for the Packet-Filter-Content AVP.

In the current release, the bidirectional filters are not allowed. That is, either the UPLINK or the DOWNLINK filter can be supported at a time. If the filter direction is detected to be bidirectional, a log is printed with the information that the bidirectional filters cannot be supported simultaneously.

CCA Result Code 4011 at MSCC Level - Behavioral Change

This Diameter-related behavioral change is applicable to all customers other than Vodafone.

In this release, the CCA result-code 4011 (DIAMETER_CREDIT_CONTROL_NOT_APPLICABLE) is allowed at the MSCC level and will cause the particular service identified by the MSCC to go offline and not the subscriber.

Default Charging Method in CCR-I Messages - Behavioral Change

This Diameter-related behavioral change is applicable to GGSN.

In StarOS 8.1, the default charging method was not being sent in CCR-I messages for dpca-custom2 (ATT dictionary), dpca-custom4 (Standard R7 Gx dictionary), and dpca-custom9 (Vf-Gx dictionary).

In this release, the default charging method is sent in CCR-I message. For this, new AVPs Online/Offline will be sent in CCR-I message based on the configuration.

Filters and Keywords in TFT-Filter AVP - Behavioral Change

This Diameter-related behavioral change is applicable to all products that use R7Gx and Gxa interfaces.

In the earlier releases, the keywords “from” and “to” were not used in the TFT-Filter AVP. Also, both UPLINK and DOWNLINK filters were supported in case of R7Gx (GGSN) and Gxa (HSGW). The TFT-Filter AVP did not use the keyword “assigned” as per RFC 3588 to indicate the address(es) assigned to the terminal.

In the current release, the keywords “from” and “to” are correctly used based on RFC 3588. Only DOWNLINK filters are supported in case of 3GPP-GPRS access types (R7Gx). The keyword “assigned” is also used correctly per RFC 3588 for all standard implementations, except for Gxa used by Verizon.

Immediate Usage Reporting Support - Behavioral Change

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

In the earlier releases, the traffic usage was not reset by PCEF after immediate reporting and the subsequent report indicated the cumulative usage.

In the current release, based on the 3GPP R9 29.212 specification, PCEF resets the usage information after immediate reporting and sends the accumulated usage since last report.

PCEF Bound Dynamic/Predefined Rules - Functional/Behavioral Change

In earlier releases, in the case of PCEF bound dynamic/predefined rules, if no MBR is configured in the charging action the rule still got installed.

In this release, ACS checks for MBR/GBR of a dynamic/predefined rule before using it for PCEF binding. All rules (dynamic as well as predefined) must have an MBR associated with them and all rules with GBR QCI must also have GBR configured. This is irrespective of R7 Gx or R8 Gx, and irrespective of GGSN or G-PGW.

Therefore, for predefined rules, appropriate peak-data-rate, committed-data-rate must be configured as per the QCI being GBR QCI or non-GBR QCI.

Policy and Charging Control Application - Behavioral Change

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

In the earlier releases, when unknown event triggers were received in the RAR command from PCRF, invalid AVP result code was set in the RAA command.

In the current release, RAR with unknown event triggers are silently ignored and responded with DIAMETER_SUCCESS.

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

This Diameter-related behavioral change is applicable to GGSN in StarOS 9.0 and later releases.

In StarOS 8.1, the QoS-Upgrade and QoS-Negotiation AVPs were not sent in CCR messages.

In the current release, if UE sets the QoS-Upgrade and QoS-Negotiation bits in CPC/UPC messages, the values are communicated to PCRF in CCR messages. New AVPs QoS-Upgrade and QoS-Negotiation will be sent in dpca-custom9 (Vf-Gx dictionary).

QoS-Class-Identifier AVP - Behavioral Change

This Diameter-related behavioral change is applicable to P-GW, HSGW, S-GW, and GGSN using R8 Gx/Gxx interface.

In the earlier releases, the QoS-Class-Identifier AVP is of type ENUM and was displayed as TRAFFIC_CLASS_A to TRAFFIC_CLASS_I for values 1 through 9 on the Diameter Gx/Gxx interface.

In the current release, based on the 3GPP TS 23.203 standard, the type value for the QoS-Class-Identifier AVP is changed to display as QCI_1 to QCI_9.

Session Level Update Notification in CCR-U Excluding Bearer Specific AVPs - Behavioral Change

This Diameter-related behavioral change is applicable to GGSN using Gx interface.

In earlier releases, the Bearer-Operation and Bearer-Identifier AVPs were sent as part of the CCR-U message with Charging Rule Report when the rule installation failures were notified.

In the current release, the Bearer-Operation and Bearer-Identifier AVPs are no longer sent in the CCR-U with Charging Rule Report which indicates PCRF that it is a session level update.

ASN GW Features in Release 10.0

This section provides information for new features in the ASN GW Service in Release 10.0.

NSP-ID and NAP-ID Functionality

NSP-ID and NAP-ID functionality enable the MS to discover all accessible network service providers (NSPs) in a WiMAX coverage area, and to indicate the NSP selection during connectivity to the ASN. The actual NSP selection by the MS may be based on various preference criteria, depending on the configuration information.

Configuration information includes:

- Information useful in the MS discovery of the network access provider (NAP), including channel center frequency and PHY profile
- Information useful in the MS decision mechanism to prioritize NSPs for automatic service selection, including a list of authorized NAPs and NSPs
- A list of authorized share or roaming relationships between authorized NAPs and NSPs and partner NAPs and NSPs
- Identity credentials provided by the NSPs to which the MS has a business relationship, and
- The mapping relation table between 24-bit NSP identities and corresponding realms of the NSPs.

Configuration information may be provided on a pre-provisioned basis or at the time of MS dynamic service subscription.

Data Tunnel Endpoint Support

ASNGW supports forwarding downlink data to different endpoint tunnels other than the control address on the BS. In addition, the ASNGW can process uplink data and control traffic on different paths (VLANs) on the ASNGW if the data and control traffic are hosted on a different IP address.

The control and data tunnel endpoint can be different for the BS or the ASNGW. If the data tunnel endpoint is different from the control endpoint, it applies for both downlink and uplink traffic destined to, or received from, the peer (BS or ASNGW). This means that when downlink traffic is sent to the peer, the data tunnel endpoint is the destination IP address; when the uplink traffic is received from this peer, the source IP address is the data tunnel endpoint. The GRE key is unique for downlink and uplink data paths.

ASNGW with a Different Tunnel Endpoint

The ASNGW supports different data tunnel points on the BS for downlink traffic. The BS conveys its data tunnel endpoint through the existing R6 TLVs within MS Info. If the uplink has a different data tunnel point, the ASNGW adds this information in the message that carries MS information, including the TLV or data path TLV that describes uplink service flow. There is a unique GRE key assigned to the uplink data path.

The ASNGW includes the tunnel endpoint TLV in the data path messages to BS or from the non-anchor GW to the anchor GW and vice-versa, to support the handoff functionality. After receiving the tunnel endpoint TLV within the data path messages, the BS forwards all the uplink data traffic to the same address.

No Handoff (INE)

For the control and data path setup for the INE, the BS/ASN specifies the different IP addresses for control and data traffic. If the ASNGW requires different data tunnel endpoints instead of control addresses, the tunnel endpoint IP address has to be populated in the MS information TLV if it is per BS for DP Reg Request/Response message.

The ASNGW creates an NPU flow using the tunnel IP address if received in the DP Reg Response message for the uplink packet. If no tunnel end point attribute is received from BS/ASNGW, by default, the control IP address is used for data traffic.

If the ASNGW requires a different data tunnel endpoint instead of a control address, the tunnel endpoint IP address is populated in the MS information TLV if it is per BS for DP Reg Request/Response message.

Inter-ASNGW Handoff

For control and data path setup for an inter-ASNGW handoff, the serving base station (SBS) is connected to the anchor GW and the target base station (TBS) is connected to the non-anchor GW. During INE, the anchor GW specifies a different IP address for data traffic. The tunnel endpoint IP address is populated in the MS information TLV in DP Reg Rsp message from non-anchor GW to the TBS. The non-anchor GW conveys the tunnel endpoint to receive the downlink traffic towards the anchor GW in the DP-Reg Req message. The anchor GW specifies the tunnel endpoint to receive the uplink traffic in the DP-Reg Rsp message.

Intra-ASNGW Handoff

For intra-ASNGW handoff, during INE, the ASNGW specifies the different data tunnel endpoint for receiving uplink traffic in the DP-Reg Req message to the serving base station (SBS). After handoff, the ASNGW specifies the different data tunnel endpoint to receive the Uplink traffic in the DP-Reg Rsp message.

Robust Header Compression (ROHC) Support

ROHC support for ASNGW calls has been implemented. Header compression is applied to ASNGW service flows when the ROHC is enabled on the ASNGW, and MS and AAA authorize ROHC for the ASNGW call.

There is also support for linking the compressor and decompressor with the ROHC parameter values negotiated over R6. In addition, there is support for sending ROHC parameters in idle mode exit messages for the ASNGW and ASNPC.

Path Modification and Dynamic SF Support

The following CLI command has been added to the asngw-service config to specify whether all the service flows should be created before the IP allocation is complete. If this CLI is not configured, during INE processing, only ISF is create with a wildcard classifier. The remaining portion is created after IP allocation.

```
[ no | default ] service-flow create-before-ip-alloc
```

Prepaid Tariff Switching Support

Tariff switching is now supported by ASNGW and WiMax HA. The WiMax prepaid accounting capability contains Available-In-Client, Volume-based, and Tariff Switching. This is useful when it is applied during peak vs. off-peak hours. This implementation includes the following:

- The PPS signals a tariff switch time by sending a prepaid tariff switch (PTS) attribute that indicates the point in time when the switch will occur.
- The PTS indicates the tariff switch interval (TSI). This represents the number of seconds from the current time.
- The PPC reports how much volume was used in total and how much volume was used after the tariff switch.
- In situations with multiple tariff switches, the PPS specifies the length of the tariff switch period using the switch functionality.

DSCP Marking Support

DSCP marking for IP packets received on an ASNGW has been implemented on a per service flow basis. The asn-qos descriptor CLI command has been enhanced to support this functionality.

ASN GW Features in Release 10.2

This section provides information for new features in the ASN GW Service in Release 10.2.

ASNGW-ID in R6 Messages

ASNGW now supports a 6-byte ASNGW-ID in the source ID TLV and destination TLV of all messages. Six-byte anchor GW and authenticator IDs are also supported in the **`peer-asngw address`** command.

Functional and Behavioral Changes

Following are some of the functional and behavioral changes as a result of the 6-byte IDs:

- Configuration of 6-byte ansgw-id in **`asngw-service`**.
- Configuration of 6-byte ID while configuring the peer-asngw address in **`asngw-service`** and **`asnpc-service`**.
- Configuration of 6-byte id while configuring the peer-asnpc address in **`asnpc-service`**.
- Sending the 6-byte ASNGW-ID and 6-byte ASNPC-ID in the source-id TLV and destination ID TLV.
- Sending the Reservation REsult in the DP Dereg Rsp if the SF-ID is present.
- Making the BS Info optional in most of the ACK messages.
- Removing the support to setting the TC bit in DSCP, CMAC Key Count TLV, etc.
- Sending the authenticator ID and anchor gateway ID as 6 bytes.

Framed Route Support on ASNGW

Framed route AAA attribute support has been added for GGSN. Theses changes have been ported to ASNGW with its support for multi-hosts (with static IP addresses) behind WiMAX CPE.

PHS Value Sent in NS Attach Response

The PHS value is now sent in the MS attach response. If PHS is not supported, the ASNGW sends a PHS TLV with a value of 0.

DP Pre-Reg Response Support

The ASNGW sends a DP Pre-Reg Response with a Data Integrity Method TLV with the value set as M. Once the Pre-Reg is complete, the ASNGW begins multi-casting.

Source and Destination ID TLVs

The ASNGW sends the source ID and destination ID TLVs in the keepalive response messages if those TLVs are received in the keepalive request.

TLVs Present in DP Dereg Rsp

For BS-initiated path Dereg, the ASNGW sends a mandatory field MS in the path Dereg Rsp message. the TLVs are present.

IPv4 CS Call Support

In addition to the “asn-policy auth-only allow” configuration or RADIUS attributes, CS Type from the BS is also considered to bring up the auth-only call. The following is the new behavior:

Auth Only from AAA or Sub Profile	CS Type	Call Type
Allow	IPv4	SIP/MIP/CMIP
Allow	802.3	Auth-Only
Disallow	IPv4	SIP/PMIP/CMIP
Disallow	802.3	Failure indicator sent in MS Attach Request

Content Filtering in Release 10.0

This section provides information on new features for Release 10.0 in the Content Filtering product.

CF-APPS Re-architecture

The Content Filtering architecture is redesigned so that the CF Application components like CDP, CCI and RE are now part of external applications, WEM and inPilot.

The CDP functionality is handled by WEM, and the RE functionality has been moved to inPilot to support the CF-EDR based reporting. The CF-CCI functionality has been eliminated on account of this redesign.

For more information, please refer to the *WEM Online Help* and *inPilot Online Help*.

ECS Features in Release 10.0

This section provides information on new features in the Active Charging Service (ACS)/Enhanced Charging Service (ECS) in Release 10.0.

Fair Usage

The Fair Usage feature enables to perform SessMgr instance-level load balancing for in-line service features, and resource usage control for subscribers. For information, refer to the feature description in the *Enhanced Charging Service Administration Guide*.

ICAP Failure Action on Re-transmitted Packets - Behavioral Change

In this release the failure-action discard behavior to be taken on re-transmitted packets when the ICAP response is not received for the original request and the retransmitted request comes in has changed. Fore more information, please refer to the *ICAP Interface Support* chapter of the *System Enhanced Feature Configuration Guide*.

X-Header Encryption

X-Header Encryption enhances the X-header Insertion feature to increase the number of fields that can be inserted, and also enables encrypting the fields before inserting them. For information, refer to the feature description in the *Enhanced Charging Service Administration Guide*.

ESS Features in Release 10.0

This section contains information on features that pertain to the Local-External Storage Server (L-ESS) and Remote (Long Term)-External Storage Server (R-ESS).

None for this release.

Firewall Features in Release 10.0

This section provides information for new features in the Stateful Firewall product in Release 10.0.

None for this release.

GGSN Features in Release 10.0

This section provides information for new features for the GGSN Service in Release 10.0.

Common Gateway Access Support

Benefits

This is a consolidated solution that combines 3G and 4G access technologies in a common gateway supporting logical services of HA, PGW, and GGSN to allow users to have the same user experience, independent of the access technology available.

Description

In todays scenarios, an operator may have multiple access networks (CDMA, eHRPD and LTE) plus a GSM/UMTS solution for international roaming. Therefore, the operator needs a solution to allow customers to access services with the same IP addressing behavior and to use a common set of egress interfaces, regardless of the access technology (3G or 4G).

This solution allows static customers to access their network services with the same IP addressing space assigned for wireless data, regardless of the type of connection (CDMA, eHRPD/LTE or GSM/UMTS). Subscribers using static IP addressing will be able to get the same IP address regardless of the access technology.

Following commands added to GGSN Service Configuration Mode for this support:

To enable system to accept duplicate call session with same IP address:

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

To enable system to allow authorization with 3GPP AAA/HSS over S6b interface:

[default] authorize-with-hss

To enable system to provide DNS query support for P-CSCF, if received from 3GPP AAA/HSS in AAA message:

dns-client context *dns_ctxt_name*
default dns-client context

To configure the FQDN for HSS address resolution:

[no | default] fqdn host *host_name* **realm** *realm_id*

For more information on this product, refer *Common Gateway Access Support* section in *GGSN Service Administration Guide*.

License Keys

Requires separate product license key.

Lawful Intercept

Lawful Intercept on the GGSN now supports the following features:

- TCP-based packet delivery format
- IPv4 and IPv6 source and destination X2 and X3 addresses
- Gn-Gp handovers

Contact your Cisco Sales Representative for more information.

GGSN Features in Release 10.2

This section provides information for new features for the GGSN Service in Release 10.2.

Address Overlapping Support for AAA/DHCP over IPSec Tunnels

Benefits

This feature enables multiple customers to send overlapping subscriber and non-subscriber (AAA and DHCP) traffic over the secured IPSec tunnels in the same context. Overlapping traffic means traffic having same source and destination address.

Description

IPSec tunnel supports AAA and DHCP address overlapping. Address overlapping is meant for multiple customers using the same IP address for AAA/DHCP servers. The AAA and DHCP control messages are sent over IPSec tunnels and AAA/DHCP packets required to be encrypted are decided as per the ACL configuration done for specific session.

Overlapping subscriber traffic works due to the fact that each IP Pool has its own IPSec Tunnel. Also each IP Pool has a unique pool-id. We utilize this fact to separate traffic streams. When an IP Pool is bound to a crypto map, an IPSec Manager is selected to establish IPSec Tunnel such that this IPSec Manager does not handle any other overlapping IP Pool IPSec Tunnel with same addresses. Once the IPSec Tunnel is established, IPSec Manager installs TX & RX NPU flows. Rx flow contains the Pool ID. Tx flow is used to transmit packets over this IPSec Tunnel. This Tx flow is sent to VPN Manager along with the IP Pool information to VPN Manager. VPN Manager stores this NPU Flow ID for this IP Pool so that it can return the Tx Flow ID when an IP Address is allocated from that Pool to the Session Manager that is going to handle subscriber traffic. Session Manager installs the regular subscriber traffic flow along with the Pool ID when overlapping IP Pools is used.

When the traffic is coming to GGSN from Internet to the subscriber over IPSec Tunnel, it matches the IPSec Rx flow (ESP flow). IP Pool id extracted from this ESP flow and a subscriber flow lookup is performed with IP Pools id after packet is decrypted.

For more information on this product, refer *Features and Functionality - Optional Enhanced Feature Software* section in *GGSN Service Administration Guide*.

License Keys

No separate license key required.

GSS Features in Release 10.0

This section provides information for new GSS features for Release 10.0

HA Features in Release 10.0

This section provides information for new features in the Home Agent product in Release 10.0.

None for this release.

HNB-GW Features in Release 10.0

This section provides information for new features in the Home-NodeB Gateway product in Release 10.0.

HNB-GW feature is new in Release 10.0.

No new feature is added for this release.

HSGW Features in Release 10.0

This section contains information on new 10.0 features that pertain to the HRPD Serving Gateway (HSGW) supporting eHRPD network services.

No new feature is added for this release.

inPilot Features in Release 10.0

This section provides information on new features in the current inPilot Release 10.0.x, which supports StarOS 9.0.

Content Filtering Reports

The Content Filtering Reporting Engine (CF-RE) reports provide the summary of traffic over Content Filtering categories, actions, and ratings.

The CF-RE report also provides the list of top N subscribers and URLs based on their unique subscriber's hit count and total usage.

Distributed Architecture of inPilot

inPilot supports the distributed model to allow the deployment which enables network wide view or work load balancing. Newly introduced component, Remote Data Processor (RDP), plays the role of pre-processing the input files from gateways. One or more RDPs, installed separately on remote machines can be registered to a master inPilot and one RDP can process files from one or more gateways.

RDP periodically sends the intermediate data to registered master inPilot. The role of inPilot in such deployments is mostly for report generation, report viewing, RDP management and optionally data processing.

IMPORTANT

For Bulkstat, there is no support for distributed model and all the bulkstat input files will be parsed by master inPilot only.

Support for E-mailing Reports

In this release, the inPilot application allows users to configure e-mail IDs and SMTP servers to send generated reports.

For more information please refer to *inPilot Installation and Administration Guide* and *inPilot Online Help*.

Weekly and Monthly Reports

In this release, inPilot supports generating weekly and monthly reports. The weekly reports provide details of the following:

- Total traffic
- Total traffic by category
- VOIP Call Duration
- Total unclassified traffic (TCP and UDP)

- Top N subscribers

The monthly reports provide the details of total traffic across the top N protocols / application categories in a month.

Password Security and Access Control Feature

The current release of inPilot allows only authenticated users to access the inPilot application. The user name and password of the inPilot user should comply to the minimum complexity requirements.

This ensures data privacy and security for inPilot at Operating System level. It also aids in preventing unauthorized access of database by end-users. Users with only certain privileges are allowed to access inPilot directories and view various reports through GUI.

DPI Report Filtering

The users can select one or more filters based on which these reports are displayed. In the current release, the following filters are supported.

- Category
- Protocol
- IP Protocol
- Radio Access Type (RAT)
- Type Allocation Code (TAC)
- Access Point Name (APN)
- Serving GPRS Support Node (SGSN)

If a single filter is selected then the graphs appear with a comparison against two groups, filter and non-filters. Also, the table displays values for filter and non-filter. If multiple filters are selected, for example, if APN and RAT filters are selected, then traffic distribution will be calculated per (selected) APN with respect to the selected RAT.

Anonymize Subscriber Data

inPilot GUI and excel report displays subscriber's private data like Mobile Station Integrated Services Digital Network (MSISDN) in encrypted format in all the subscriber-based reporting.

Users with administrative privilege can only decrypt the MSISDNs using a shell script utility. For information on how to use this script, see the *inPilot Installation and Administration Guide*.

This feature is available only with the fresh installation.

Support for Unknown URLs

For CF reporting, inPilot should parse CF-EDRs and generate the unknown/unrated URL database. This database will be pulled periodically by WEM and subsequently deliver to Rulespace. The unknown URL files can either be time based or URL count based.

IP Services Gateway Features in Release 10.0

This section provides information for new features in the IP Services Gateway product.

None for this release.

NAT Features in Release 10.0

This section contains information for new features in the Network Address Translation (NAT) product in Release 10.0.

NAT ALG Support

This release supports NAT Application Level Gateways (ALGs) for the following protocol:

- Point-to-Point Tunneling Protocol (PPTP)
- Session Initiation Protocol (SIP)
- Trivial File Transfer Protocol (TFTP)

For more information, please refer to the *Network Address Translation Administration Guide*.

NAT IP Pool Group Support

This release supports grouping of NAT IP pools.

Similar NAT pools can be grouped into NAT IP pool groups. This enables to bind discontiguous IP address blocks in individual NAT IP pools to a single NAT pool group.

When configuring a NAT pool group, note that only those NAT pools that have similar characteristics can be grouped together. The similarity is determined by the NAT Pool Type (One-to-One / Many-to-One), users configured per NAT IP address (applicable only to Many-to-one NAT pools), NAT IP Address Allocation Mode (On-demand/Not-on-demand), and Port Chunk Size (applicable only to Many-to-one NAT pools) parameters.

IMPORTANT

Dissimilar NAT pools cannot be grouped together.

It is recommended that for each NAT pool in a NAT pool group the other parameters also be configured with the same values, so that the NAT behavior is predictable across all NAT pools in that NAT pool group.

The NAT pool from which a NAT IP address is assigned will determine the actual values to use for all parameters.

It is recommended that in a Firewall-and-NAT policy all the realms configured either be NAT pools or NAT pool groups. If both NAT pool(s) and NAT pool group(s) are configured, ensure that none of the NAT pool(s) are also included in the NAT pool group.

For more information, please refer to the *Network Address Translation Administration Guide*.

NAT Binding Records

This release supports the following new NBR attributes that are applicable to PGW and GGSN:

- bearer 3gpp charging-id
- bearer 3gpp sgsn-address
- bearer ggsn-address

The following NBR attributes are not applicable to PGW and GGSN:

- sn-correlation-id
- sn-fa-correlation-id
- radius-fa-nas-ip-address
- radius-fa-nas-identifier

For more information, please refer to the *Network Address Translation Administration Guide*.

PDIF Features in Release 10.0

This section provides information for new features in the Packet Data Interworking Function.

Session Counting License

In Release 10.0, the PDIF is a licensed product with a session counting license, which can be purchased in 1,000 or 10,000 session increments. For information about PDIF licenses, contact your sales representative.

PSC2 Support

In Release 10.0, the PDIF supports the Packet Services Card 2 (PSC2). The PSC2 is the next-generation packet forwarding card for the ASR 5000. The PSC2 provides increased aggregate throughput and performance, and a higher number of subscriber sessions.

Multiple PDIF Services

In Release 10.0, the PDIF supports multiple PDIF services running simultaneously on the same ASR 5000. This feature enables operators to configure PDIF services with different crypto templates to support multiple subscriber handsets and to set per-service maximum session limits. The total number of sessions for all PDIF services running simultaneously on the same ASR 5000 must fall under the PDIF session counting license limit.

Packet Data Gateway/Tunnel Termination Gateway Features in Release 10.0

This section provides information for new features in the Packet Data Gateway/Tunnel Termination Gateway (PDG/TTG) Features in Release 10.0.

Lawful Intercept

In Release 10.0, the TTG supports lawful interception (LI) of subscriber session information to provide telecommunication service providers (TSPs) with a mechanism to assist law enforcement agencies (LEAs) in the monitoring of suspicious individuals (referred to as targets) for potential criminal activity.

IMS Emergency Call Handling

In Release 10.0, the PDG/TTG supports IMS emergency call handling per 3GPP TS 33.234. This feature is enabled by configuring a special WLAN access point name (W-APN), which includes a W-APN network identifier for emergency calls (sos, for example), and can be configured with no authentication.

The DNSs in the network are configured to resolve the special W-APN to the IP address of the PDG/TTG. When a WLAN UE initiates an IMS emergency call, the UE sends a W-APN that includes the same W-APN network identifier (sos) as the one that is configured on the PDG/TTG. This W-APN network identifier is prefixed to the W-APN operator identifier per 3GPP TS 23.003. The W-APN operator identifier sent by the UE must match the PLMN ID (MCC and MNC) that is configured on the PDG/TTG (visited network). When the PDG/TTG receives the W-APN from the UE in the IDr, the PDG/TTG marks the call as an emergency call and proceeds with call establishment, even in the event of an authentication or EAP failure from the AAA/EAP server.

If the PDG/TTG detects that an old IKE SA for the special W-APN already exists, it deletes the IKE SA and sends an INFORMATIONAL message with a Delete payload to the WLAN UE to delete the old IKE SA on the UE.

IPSec Session Recovery Support

In Release 10.0, the session recovery feature is a licensed feature. It provides seamless failover and nearly instantaneous reconstruction of subscriber session information in the event of a hardware or software fault within the same chassis, preventing a fully-connected user session from being dropped. For information about the required software license for this feature, contact your sales representative.

Session recovery is performed by mirroring key software processes (the IPSec manager, session manager, and AAA manager, for example) on the PDG/TTG. These mirrored processes remain in an idle state (in standby mode), where they perform no processing until they may be needed in the case of a software failure (a session manager task aborts, for example). The system spawns new instances of standby mode sessions and AAA managers for each active control processor being used.

PDN Gateway Features in Release 10.0

This section contains information on new 10.0 features that pertain to the eGTP PDN Gateway (P-GW) supporting LTE network services.

Gy Support

The Gy interface provides a standardized Diameter interface for real time content based charging of data services. It is based on the 3GPP standards and relies on quota allocation. It is the connection between the P-GW and an On-line Charging Server.

The following Online Charging models and functions are supported:

- Time based charging
- Volume based charging
- Volume and time based charging
- Final Unit Indication and termination or redirection of service data flows when quota is consumed
- Reauthorization triggers to rearm quotas for one or more rating groups using multi-service credit control (MSCC) instances
- Event based charging
- Billing cycle bandwidth rate limiting
- Fair usage controls

Lawful Intercept Support

In accordance with 3GPP TS 33.108 Release 8 requirements, the Cisco P-GW supports the Lawful Intercept Access Function for intercepting control and data messages of mobile targets.

The Cisco P-GW provides access to the intercepted Content of Communications (CC) and the Intercept Related Information (IRI) of the mobile target and services related to the target on behalf of Law Enforcement Agencies. In this release the P-GW supports the following three interfaces:

- X1 provisioning interface from Administrative Function (ADMF) using CLI over SSH
- X2 event delivery interface for transferring Intercept Related Information (IRI) to a Delivery Function/Mediation server
- X3 content delivery

In addition, the P-GW also supports call type handling and Gn-Gp Handovers.

Contact your Cisco sales representative for more information.

VLAN Tagging Support

P-GW now supports Virtual LANs (VLANs) which provide greater flexibility in the configuration and use of contexts and services.

VLANs are configured as “tags” on a per-port basis and allow more complex configurations to be implemented. The VLAN tag allows a single physical port to be bound to multiple logical interfaces that can be configured in different contexts. Therefore, each Ethernet port can be viewed as containing many logical ports when VLAN tags are employed.

For more information on VLAN support, refer to the VLANs chapter in the *System Enhanced Feature Configuration Guid*e.

IPv6 Support on S5/S8 Interface

The eGTP P-GW now supports IPv6 transport for tunneling and management on the S5/S8 interface to/from the Serving Gateway.

IPv6 Pool Support in P-GW Pool Groups

The P-GW now supports:

- Assignment of IPv6 prefix by using pool group in APN configuration
- Even distribution of IPv6 prefix assignments from multiple IPv6 prefix pools which fall under the same pool group
- Assignment of IPv6 prefix pools and IPv4 addresses from multiple pools which share the same pool group name

PDSN Features in Release 10.0

This section provides information for new features in the Packet Data Serving Node in Release 10.0.

None for this release.

Peer-to-Peer Features in Release 10.0

This section provides information for new features for Release 10.0 in the in-line Peer-to-Peer support.

P2P Voice Call Duration

The P2P product has the capability to detect network traffic created by P2P VoIP clients such as Skype, Yahoo, MSN, Gtalk, Oscar. The VoIP call duration is a direct indication to the revenue impact of the network operator. The P2P product is well poised to process the network traffic online to detect and control the VoIP presence, and generate records that can be used to calculate the VoIP call durations.

For more information, please refer to the *Peer-to-Peer Overview* chapter in the *Peer-to-Peer Detection Administration Guide*.

Random Drop Charging Action

The random drop charging action is added as an option to degrade P2P voice calls. This is achieved by randomly dropping packets of the voice calls over the voice call period. Voice data is encoded in multiple packets by the codec. Since there is a possibility of packets being dropped in a network, the codec replicates the same information across multiple packets. This provides resilience to random packet drops in the network. For a considerable degradable voice quality, a chunk of packets need to be dropped. By this way, the codec will be unable to decode the required voice information. The chunk size for achieving degradation of voice call varies from one protocol to another.

For more information, please refer to the *Peer-to-Peer Overview* chapter in the *Peer-to-Peer Detection Administration Guide*.

New Protocols

The P2P solution now detects the following new protocols:

- ActiveSync
- Aimini
- Battlefield
- Freenet
- IAX
- IPTV
- Nimbuzz
- OpenFT
- Paltalk
- Pandora
- QQgame
- Quake

- RDP
- SecondLife
- Warcraft3

For more information, please refer to the *Peer-to-Peer Detection Administration Guide*.

Session Control Manager Features in Release 10.0

This section provides information for new features in Release 10.0 for the Session Control Manager (SCM). Additional information on these features can be found in the *Session Control Manager Overview* section of the *Product Overview*, in the *Session Control Manager Administration Guide*, and in the *CLI Reference Guide*.

IMS Architecture

Interrogating-CSCF

The I-CSCF can now be incorporated into the Serving-CSCF only. There are no longer any I-CSCF features supported by an integrated Proxy/I-CSCF.

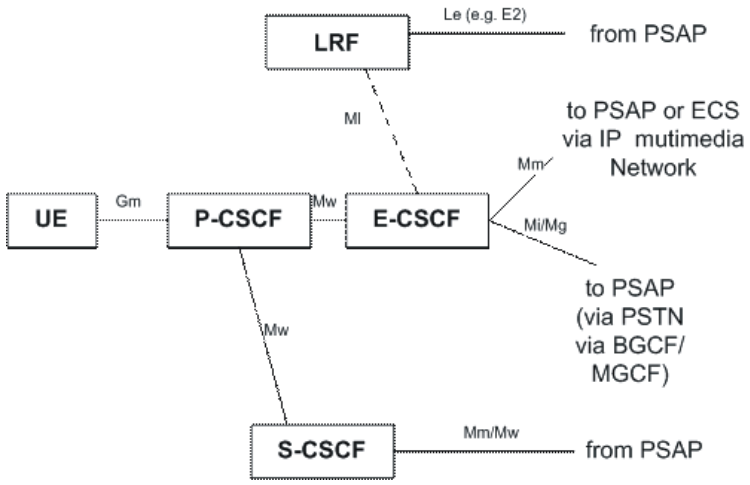
Emergency-CSCF Supported

The Emergency-CSCF (E-CSCF) is a network element in IMS which is responsible for routing an emergency call to a Public Safety Answering Point (PSAP).

To identify the next hop PSAP, E-CSCF interacts with the Location Retrieval Function (LRF). LRF provides the necessary routing information so that E-CSCF can route the request to the appropriate PSAP.

E-CSCF Interfaces

The following diagram shows the interfaces/reference points associated with the E-CSCF:



SIP Interfaces

MI - The reference point between the E-CSCF and Location Retrieval Function (LRF). The MI interface is used for routing an emergency call to a Public Safety Answering Point (PSAP). The E-CSCF interacts with the Location Retrieval Function (LRF) to identify the next hop PSAP.

New Features and Functionality - Base Software

Call Types Supported

The following new call type is supported:

- **Emergency calls** - are managed through the addition of an Emergency Call/Session Control Function (E-CSCF) that routes emergency calls to a Public Safety Answering Point (PSAP).

Emergency Call Support

P-CSCF gives priority to emergency calls, especially in a congested network. In addition, P-CSCF rejects new calls to any user who is in an emergency call.

MSRP Support

The SCM supports Message Session Relay Protocol (MSRP) session and page modes.

Shared Initial Filter Criteria (SiFC)

If both the HSS and the S-CSCF support this feature, subsets of iFC may be shared by several service profiles. The HSS downloads the unique identifiers of the shared iFC sets to the S-CSCF. The S-CSCF uses a locally administered database to map the downloaded identifiers onto the shared iFC sets.

If the S-CSCF does not support this feature, the HSS will not download identifiers of shared iFC sets.

New Features and Functionality - Licensed Enhanced Feature Support

IPv4-IPv6 Interworking

MSRP is now supported when IPv4-IPv6 interworking is enabled.

IPv6 Support

In addition to supporting IPv4, the SCM supports IPv6 addressing. A CSCF service can be configured with v6 addresses to support an all v6 network.

IMPORTANT

For this feature, you may bind a CSCF service to either an IPv4 address or to an IPv6 address, but not both simultaneously.

Lawful Intercept

The SCM CSCF service now supports Call Content and Interception for the Lawful Intercept feature.

Contact your Cisco Sales representative for more information.

Supported Standards

The SCM service now complies with the following standards for CDMA2000 PDSN and UMTS GGSN network wireless data services.

Release 8 3GPP References

IMPORTANT

The SCM currently supports the following Release 8 3GPP specifications. Most 3GPP specifications are also used for 3GPP2 support; any specifications that are unique to 3GPP2 would be listed under Release 8 3GPP2 References.

- TS 23.167 IP Multimedia Subsystem (IMS) emergency sessions
- TS 24.229 IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3
- TS 29.214 Policy and charging control over Rx reference point
- TS 33.178 Security aspects of early IP Multimedia Subsystem (IMS)
- TS 33.978 Security aspects of early IP Multimedia Subsystem (IMS)

SGSN Features in Release 10.0

This section describes the features available with SGSN release 10.0.

Lawful Intercept

The Lawful Intercept feature now supports the following features:

- Application Heartbeat Messages
- Short Message Service MO and MT

Contact your Cisco sales representative for more information.

Serving Gateway Features in Release 10.0

This section contains information on new 10.0 features that pertain to the eGTP Serving Gateway (S-GW) supporting LTE network services.

Session Recovery Support

The S-GW now provides seamless failover and reconstruction of subscriber session information in the event of a hardware or software fault within the system, preventing a fully connected user session from being disconnected.

IPv6 Support for S5/S8 Interface

The eGTP S-GW now supports IPv6 transport for tunneling and management on the S5/S8 interface to/from the PDN Gateway.

IPv6 Support for S11 and S1-U Interfaces

The eGTP S-GW now supports IPv6 transport for tunneling and management on the S11 and S1-U interfaces to/from the MME and eNodeB respectively.

Lawful Intercept

The S-GW now supports the following Lawful Intercept features:

- IPv6 source and destination X2 and X3 addresses
- Call Type handling

Contact your Cisco Sales Representative for more information.

Web Element Manager Features in Release 10.0

This section provides information for new features for the Web Element Manager application in Release 10.0.

Bulk Statistics Enhancements

The following schema categories have been enhanced with additional bulk statistics:

- PGW
- LMA
- BCMCS
- DIAMETER
- DCCA
- DPCA
- NAT
- IMSA
- ECS
- GTPC
- SGTP
- GPRS
- SGSN
- CSCF
- Context
- Card

Refer to the Accounting Management chapter in this Change Reference a list of the new bulk statistics.

Database Migration Support During WEM Upgrade

WEM now supports database migration during a WEM upgrade. During the upgrade, the WEM Server data migration script checks if the system has an older version of POSTGRES. If the script finds the installed POSTGRES version older than the POSTGRES in the new version being installed, it starts the database migration process.

The database migration process runs in the background while WEM is upgraded. After the WEM upgrade is complete, the user can begin working in WEM and check on the progress of the data migration.

Support for Aggregate Audit Attributes

WEM now supports aggregating multiple audit attributes into a single attribute through the use of mathematical operators. These aggregate audit attributes are then available for use with the Configuration Audit feature.

For more information on this feature, refer to the Security Management chapter in this reference.

Support for Field Separators When Defining Audit Attributes

WEM now supports the parsing of audit attributes for the Configuration Audit feature by using a using a user-defined field separator and secondary field separators

For more information on this feature, refer to the Security Management chapter in this Change Reference.

Support for Additional Email Configuration of Audit Report Distribution

WEM now supports the editing of the configuration audit report's email title and body.

For more information on this feature, refer to the Security Management chapter in this Change Reference.

Validation of Configuration Audit Attributes

WEM now supports the validation of audit attribute results against a user-defined value for use with the Configuration Audit feature.

For more information on this feature, refer to the Security Management chapter in this Change Reference.

CSCF Parameters Support for Subscriber Configuration

WEM supports the configuration of Call Session Control Function (CSCF) parameters to be used with a subscriber configuration. For more information, refer to the Configuration Management chapter in this Change Reference.

Support for the WEM Identifier Feature

WEM now provides a feature that enables the user to enter a unique WEM Identifier text string upon login that will appear at the top of every WEM screen opened during a user session. The WEM Identifier text can be used to differentiate between multiple WEM sessions opened by individual users. For more information, refer to the Configuration Management chapter in this Change Reference.

Enhancement to getSupportDetails.pl

The WEM getSupportDetails.pl script has been enhanced to allow the user to specify the output directory for the emssupportDetails.tar.gz file if the output directory is different from the default output directory (/tmp/).

For more information, refer to the Configuration Management chapter in this Change Reference.

Windows 7 Support for WEM

WEM now can be accessed by client machines running the Windows 7 operating system.

For more information, refer to the Configuration Management chapter in this Change Reference.

Enhancement to WEM Server nms.cfg File

The WEM Server *nms.cfg* file has been enhanced to allocate an additional ServerIIOPPort for ASR 5000 to WEM server callback information. For more information, refer to the Configuration Management chapter in this Change Reference.

DNS Client Information Support for IMS

WEM now provides performance information for IMS DNS clients. Information can be obtained by System and context, query type, query name, and client name.

For more information, refer to the Performance Management chapter in this Change Reference.

CHAPTER 2
FAULT MANAGEMENT

This section contains additions and changes made to the fault management features available in Release 10.0.

SNMP MIB Objects in Release 10.0

This section lists the MIB objects and alarms new / modified in Release 10.0.

New Objects

- starNPUSlot
- starThreshNPUUtilization
- starThreshClearNPUUtilization
- starThreshDnsLookupFailure
- starThreshClearDnsLookupFailure
- starThreshDiameterRetryRate
- starThreshClearDiameterRetryRate
- starGSServiceStart
- starGSServiceStop
- starMAPServiceStart
- starMAPServiceStop
- starIUPSServiceStart
- starIUPSServiceStop
- starSGTPServiceStart
- starSGTPServiceStop
- starSlotPartNumber
- starSlotPartRevision
- starSlotSerialNumber
- starSlotCLEICode
- starSlotCiscoModelName
- starSlotCiscoHardwareRev
- starSlotCiscoSerialNumber

Modified Objects

None for this release.

Obsoleted Objects

None for this release.

Deleted Objects

None for this release.

New Alarms

None for this release.

Modified Alarms

None for this release.

Obsoleted Alarms

None for this release.

Deleted Alarms

None for this release.

Web Element Manager Path

Select Configuration | SNMP Configuration.

Content Filtering MIB Objects for Release 10.0

This section lists the Content Filtering MIB objects and alarms new/modified in Release 10.0.

New Objects

None for this release.

Modified Objects

None for this release.

Obsoleted Objects

None for this release.

Deleted Objects

None for this release.

New Alarms

None for this release.

Modified Alarms

None for this release.

Obsoleted Alarms

None for this release.

Deleted Alarms

None for this release.

Web Element Manager Path

Select Configuration | SNMP Configuration.

ESS MIB Objects for Release 10.0

This section lists the new and modified MIB objects and alarms for Local-External Storage Server (L-ESS) in Release 10.0.

New Objects

None for this release.

Modified Objects

None for this release.

Obsoleted Objects

None for this release.

Deleted Objects

None for this release.

New Alarms

None for this release.

Modified Alarms

None for this release.

Obsoleted Alarms

None for this release.

Deleted Alarms

None for this release.

Intelligent Packet Monitoring Systems (IPMS) MIB in Release 10.0

This section lists the new and modified MIB objects and alarms for IPMS in Release 10.0.

New Objects

None for this release.

Modified Objects

None for this release.

Obsoleted Objects

None for this release.

Deleted Objects

None for this release.

New Alarms

None for this release.

Modified Alarms

None for this release.

Obsoleted Alarms

None for this release.

Deleted Alarms

None for this release.

Web Element Manager Path

Select Configuration | SNMP Configuration.

Web Element Manager Enhancements in Release 10.0

This section contains new and modified MIB objects and alarms for Web Element Manager. in Release 10.0.

New Objects

None for this release.

Modified Objects

None for this release.

Obsoleted Objects

None for this release.

Deleted Objects

None for this release.

New Alarms

None for this release.

Modified Alarms

None for this release.

Obsoleted Alarms

None for this release.

Deleted Alarms

None for this release.

Web Element Manager Path

Select Configuration | SNMP Configuration.

CHAPTER 3
CONFIGURATION MANAGEMENT

This section contains additions and changes made to the configuration commands available in Release 10.0. Topics covered in this chapter are:

New Configuration Commands

This section contains configuration commands that are new in Release 10.0. New commands in this version are divided into the following sections:

Common Commands - New in Release 10.0

This section provides information on new commands that are common to products in Release 10.0.

diameter mscc-final-unit-action terminate

This command is added to support termination of PDP session or category based on the First-Unit-Action (FUA) in a particular MSCC and the quota exhaustion for that service.

CLI (Credit Control Configuration Mode)

```
diameter mscc-final-unit-action terminate { category | session {
on-per-mscc-exhaustion | on-all-mscc-exhaustion } }

default diameter mscc-final-unit-action terminate { category | session {
on-per-mscc-exhaustion | on-all-mscc-exhaustion } }
```

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

event update

This command enters the Policy Control Configuration mode for Diameter Policy Control Application (DPCA) to send the volume usage information when the event change is reported to PCRF in CCR-U message..

CLI (IMS Authorization Service Configuration Mode)

```
[ no | default ] event-update send-usage-report
```

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

mpls bgp forwarding

New command added to support dynamic MPLS label on BGP. This command globally enables the MPLS BGP forwarding. By enabling this command, the BGP VPNv4 routes need not have an underlying LDP LSP to forward the IP packets.

CLI (Context Configuration Mode)

```
[no] mpls bgp forwarding
```

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

vsa-support

This command allows database to use the vendor IDs from the dictionary or the supported vendor IDs that satisfy capabilities negotiation.

CLI (Diameter Endpoint Configuration Mode)

```
vsa-support{ all-from-dictionary | negotiated-vendor-ids }

default vsa-support
```

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

ASN GW Commands - New in Release 10.0

This section provides information on new ASN GW commands available in Release 10.0.

asn-header-compression rohc

This command is added to negotiate robust header compression support for subscribers with AAA for WiMax calls. This configuration indicates the type of header compression enabled on the ASNGW. NAS uses this configuration to indicate and pack ROHC support sub TLV in the WiMAX-Capability attribute in the Access-Request message. The ROHC header compression is applied only when ROHC is supported on ASNGW, and ROHC support is indicated in AAA. The default value is disabled.

CLI (Subscriber Configuration Mode)

```
[ no | default ] asn-header-compression rohc
```

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

asn nspid

This configuration command is added to specify the NSP associated with WiMax subscribers. If configured, the NSP ID is sent in Access-Request and Accounting messages. By default, NO NSP ID is configured in the subscriber template.

CLI (Subscriber Configuration Mode)

```
asn nspid <id>
```

Where <id> is the 3-byte NSP ID in HEX format, such as FF-EE-01.

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

asn-service-profile id

This command is added to asn-service-profile to configure the activation trigger for that asn-service-profile. The default value is **provisioned | admit | activate.**

CLI (ASN Service Profile Configuration Mode)

```
asn-service-profile id <id> direction {bi-directional | uplink | downlink }
[activation-trigger (activate | admit | dynamic-reservation |
provisioned)*]
```

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

create-before-ip-alloc

This command specifies whether all the service flows should be created before the IP allocation is complete. If this command is not configured, during the INE process, only ISF is created with a wildcard classifier. The remaining is created after the IP allocation. The default value is disabled.

CLI (Service Flow Configuration Mode)

`create-before-ip-alloc`

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

header-compression rohc

This command is added in the asngw-service to configure ROHC support and parameters. If ROHC is supported on the asngw-service, ROHC support is indicated in the MS attachment messages, if ROHC is authorized for the particular SF. The default value is disabled.

CLI (ASNGW Service Configuration Mode)

`[no | default] header-compression rohc`

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

local-data-tunnel address

This command specifies the tunnel endpoint on the ASNGW side that receives the uplink data packet over the R6 interface. This address is different from the R6 control address.

CLI (Service Configuration Mode)

`local-data-tunnel address <IPv4>`

where **`<IPv4>`** is the IP address to receive the uplink data traffic.

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

ASN GW Commands - New in Release 10.2

This section provides information on new ASN GW commands available in Release 10.2.

asngw-id

This configuration command enhances the existing CLI for configuring a 6-byte ID for the peer ASNGW service.

CLI (ASNGW Service Configuration Mode)

```
asngw-id <6-byte MAC address>
```

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

peer-asngw address

This configuration command enhances the existing CLI for configuring a 6-byte ID for the peer ASNGW service.

CLI (ASNGW Service Configuration Mode)

For an ASNGW service:

```
peer-asngw address <ipv4-address> [id < 6-byte MAC address > |mode {legacy
| non-legacy} | simple-ip re-achoring ]*
```

For an ASNPC service:

```
peer-asngw address <value> [id < MAC > | mode [ legacy | non-legacy ]]
```

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

Content Filtering Commands - New in Release 10.0

This section provides information on new commands available in Release 10.0.

None for this release.

ECS Commands - New in Release 10.0

This section provides information on new ECS commands available in Release 10.0.

edr-udr-flow-control

This command enables Flow Control between Session Managers and the CDRMOD process.

CLI (Context Configuration Mode)

edr-udr-flow-control [unsent-queue-size *queue_size* **]**

{ default | no } edr-udr-flow-control

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

fair-usage

This command enables Fair Usage feature and enables configuring Fair Usage parameters.

CLI (Active Charging Service Configuration Mode)

fair-usage [deact-margin *deactivate_margin* **| threshold-percent** *usage_threshold* **]**

default fair-usage [deact-margin | threshold-percent]

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

fair-usage session-waiver-percent

This command configures a waiver on top of average available memory credits per session for the Fair Usage feature.

CLI (Rulebase Configuration Mode)

fair-usage session-waiver-percent *waiver_percent*

default fair-usage session-waiver-percent

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

http attribute-in-data

This command enables configuring dynamic header field in application payload.

CLI (Ruledef Configuration Mode)

[no] http attribute-in-data *field_name* **[case-sensitive]** *operator string*

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

http attribute-in-url

This command enables configuring dynamic header field in URL.

CLI (Ruledef Configuration Mode)

[no] http attribute-in-url *field_name* **[case-sensitive]** *operator string*

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

xheader-encryption

This command enables configuring dynamic header field in URL.

CLI (Rulebase Configuration Mode)

xheader-encryption { certificate-name *certificate_name* **| re-encryption period** *reencryption_period* **}**

default xheader-encryption re-encryption period

no xheader-encryption { certificate-name | re-encryption }

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

Firewall Commands - New in Release 10.0

This section provides information on new commands available in Release 10.0.

GGSN Commands - New in Release 10.0

This section provides information on new commands available in Release 10.0.

authorize-with-hss

New command added to support the S6b interface on GGSN for authorization with 3GPP AAA/HSS to provide session interoperability with P-GW and HA.

CLI (GGSN Service Configuration Mode)

`[default] authorize-with-hss`

IMPORTANT

This is a license-enabled command.

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

dns-client

New command added to define the context name where a DNS client is configured. This command will associates an existing DNS client configuration with GGSN to perform DNS query for P-CSCF, if P-CSCF query request in AAA message is received from Diameter node.

CLI (GGSN Service Configuration Mode)

`dns-client context` *`dns_ctxt_name`*

`[no] dns-client context`

IMPORTANT

This is a license-enabled command.

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

fqdn

New command added to define the Fully Qualified Domain Name (FQDN) which would be used for authorization over S6b interface between GGSN and 3GPP AAA/HSS.

CLI (GGSN Service Configuration Mode)

`[no | default] fqdn host` *`host_name`* **`realm`** *`realm_id`*

IMPORTANT

This is a license-enabled command.

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

newcall

New command added to enable/disable the new call related behavior of GGSN service when duplicate sessions with same IP address request is received. This feature is required to support the interworking with P-GW and HA.

CLI (GGSN Service Configuration Mode)

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

IMPORTANT

This is a license-enabled command.

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

HA Commands - New in Release 10.0

This section provides information on new commands available in Release 10.0.

None for this release.

HNB-GW Commands - New in Release 10.0

This section provides information on new commands available in Release 10.0.

HNB-GW service is new in Release 10.0.

Several configuration mode and commands added/modified for this service.

hnbgw-service

The HNB-GW is new in Release 10.0.

New service mode added for HNB-GW service configuration.

CLI (Context Configuration Mode)

`[no] hnbgw-service` *`hnbgw_svc_name`* **`[-noconfirm]`**

IMPORTANT

This is a license-enabled service.

With this release, Cisco Systems introduced Home-NodeB Gateway. The Home NodeB Gateway is the HNB network access concentrator used to connect the Home NodeBs (HNBs)/Femto Access Point (FAP) to access the UMTS network through HNB Access Network. It aggregates Home Node-B or Femto Access Points to a single network element and then integrates them into the Mobile Operators Voice, Data and Multimedia networks.

Multiple configuration modes and commands added for this feature in Command Line Interface Reference. For more information on this product, refer *HNB Gateway Administration Guide*.

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

NAT Commands - New in Release 10.0

This section provides information on new NAT commands available in Release 10.0.

None in this release.

PDIF Commands - New in Release 10.0

This section provides information on new commands available in Release 10.0.

None for this release.

PDN Gateway Commands - New in Release 10.0

This section provides information on new P-GW commands available in Release 10.0.

fqdn

Configures a Fully Qualified Domain Name for this P-GW service used in messages between the P-GW and a 3GPP AAA server over the S6b interface.

CLI (P-GW Service Configuration Mode)

`fqdn host` *`domain_name`* **`realm`** *`realm_name`*

`[ default | no ] fqdn`

gx-li context

Configures the name of the context where lawful intercept packets are delivered to the lawful intercept server.

CLI (P-GW Service Configuration Mode)

`gx-li context` *`name`*

`default gx-li context`

newcall

Configures the P-GW to accept or reject requests for a static IP address if the address is already in use by another session.

CLI (P-GW Service Configuration Mode)

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

`no newcall duplicate-subscriber-requested-address`

PDSN Commands - New in Release 10.0

This section provides information on new commands available in Release 10.0.

None for this release.

Peer-to-Peer - New in Release 10.0

This section provides information on new Peer-to-Peer commands in Release 10.0.

None for this release.

Serving Gateway Commands - New in Release 10.0

This section provides information on new S-GW commands available in Release 10.0.

None for this release.

Session Control Manager Commands - New in Release 10.0

This section provides information on new commands available in Release 10.0.

cscf last-route-profile

Creates a last route profile, which will be specified on peer server configuration to select the Last Routing Option (LRO) number while forwarding an emergency call packet to a particular peering server, and enters the Last Route Profile Criteria Configuration Mode.

CLI (Context Configuration Mode)

cscf last-route-profile name *profile_name* **criteria { county-name | round-robin } [-noconfirm]**

no cscf last-route-profile name *profile_name*

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

privacy

Enables privacy support on the E-CSCF.

CLI (CSCF Emergency-CSCF Configuration Mode)

[no | default] privacy

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

county-name

Configure county names and assign them Last Routing Option (LRO) numbers to be used by the CSCF last route profile.

CLI (CSCF Last Route Profile Criteria Configuration Mode)

county-name *county_name* **lro-number** *value*

[no] county-name *county_name*

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

lro-number

Configure the Last Routing Option (LRO) numbers to be used by the CSCF last route profile.

CLI (CSCF Last Route Profile Criteria Configuration Mode)

[no] lro-number *value*

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

lro-selection-profile

Binds a CSCF last route profile with the peer server.

CLI (CSCF Peer Server Monitoring Configuration Mode)

lro-selection-profile name *profile_name*

no lro-selection-profile

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

peer-sbc

Configures peer Session Border Controller (SBC) addresses from where the P-CSCF/A-BG service can receive requests.

CLI (CSCF Proxy-CSCF Configuration Mode)

[no] peer-sbc *ip_address*

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

reliable-prov-resp

Enables/disables the reliability of provisional responses feature.

CLI (CSCF Proxy-CSCF Configuration Mode)

reliable-prov-resp { mandatory | optional }

[no] reliable-prov-resp

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

restoration-procedure

Enables the P-CSCF/A-BG service to reject with a 504 response when it receives 3xx, 480, or “no response” to service request. This feature is disabled by default.

CLI (CSCF Proxy-CSCF Configuration Mode)

[no] restoration-procedure

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

emergency-cscf

Enables the Emergency-CSCF for the service and enters the Emergency-CSCF Configuration Mode. Default is disabled.

CLI (CSCF Service Configuration Mode)

[no] emergency-cscf

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

media-bridging

Enables SDP modification that terminate media on CSCF. Feature is disabled by default.

CLI (CSCF Service Configuration Mode)

[no] media-bridging

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

serving-cscf-list

Configure a list of Serving CSCFs and their capabilities.

CLI (CSCF Service Configuration Mode)

[no] serving-cscf-list server { address *address* **| domain** *domain* **}**
{ capability *value* **| port** *num* **{ capability** *value* **} }**

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

3gpp

Enables/disables functionality related to 3GPP Release 8 support. This command is disabled by default.

CLI (CSCF Serving-CSCF Configuration Mode)

[default | no] 3gpp Rel8

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

alias-indication

Enables/disables alias indication functionality, a collaborative information exchange between the S-CSCF and HSS. This command is disabled by default.

CLI (CSCF Serving-CSCF Configuration Mode)

[default | no] alias-indication

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

ims-restoration

Enables/disables IMS restoration procedures. This feature is disabled by default.

CLI (CSCF Serving-CSCF Configuration Mode)

`[ default | no ] ims-restoration`

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

local-call-features

Enables/disables local call features. This command is disabled by default.

CLI (CSCF Serving-CSCF Configuration Mode)

`[ default | no ] local-call-features`

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

network-id

Configures the Network Identifier.

CLI (CSCF Serving-CSCF Configuration Mode)

`network-id` *`id`*

`[ no ] network-id`

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

sip-header

Enable SIP P-User-Database (PUD) header insertion for the S-CSCF service.

CLI (CSCF Serving-CSCF Configuration Mode)

`[ no ] sip-header insert p-user-database`

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

alias-indication

Enables/disables alias indication functionality, a collaborative information exchange between the CSCF and HSS. This command is disabled by default.

CLI (CSCF SIP Proxy Configuration Mode)

`[ default | no ] alias-indication`

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

ims-restoration

Enables/disables IMS restoration procedures. This feature is disabled by default.

CLI (CSCF SIP Proxy Configuration Mode)

```
[ default | no ] ims-restoration
```

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

Modified Configuration Commands

This section contains configuration commands that have been modified in Release 10.0. Modified commands in this version are divided into the following sections:

Common Commands - Modified in Release 10.0

This section provides information on common commands modified for Release 10.0.

route-target

New keyword **`import`** and **`both`** added to configure the import route targets and also to configure both, import and export simultaneously.

CLI (Border Gateway Protocol IP VRF Configuration Mode)

`[no] route-target {both | export | import}` **{***`asn_value`* **|** *`ip_address`***}** *`rt_value`*

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

ip maximum-routes

Number of maximum routes in IP VRF is increased to 16834 from 10000 in this command.

CLI (IP VRF Configuration Mode)

[no] ip maximum-routes *ip_route_value*

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

router

New keyword **ospfv3** added to the router command which allows to enter the ipv6 OSPF configuration mode.

CLI (Context Configuration Mode)

[no] router {ospf | bgp *as_number* **| ospfv3} Web Element Manager Path**

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

Content Filtering Commands - Modified in Release 10.0

This section provides information on Content Filtering commands modified in Release 10.0.

ECS Commands - Modified in Release 10.0

This section provides information on ECS commands modified in Release 10.0.

attribute

This command specifies the order of fields in the EDR. The following options were added to this command:

- sn-fa-ip-address

CLI (UDR 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] | [{ bytes | pkts } { downlink | uplink }]] priority** *priority* **}**

no attribute *attribute* **[priority** *priority* **]**

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

bearer

The following options have been deprecated from bearer and added within 3gpp:

- apn
- imsi
- rat-type
- sgsn-address

CLI (X-Header 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 | radius-calling-station-id | session-id | sn-rulebase | subscriber-ip-address | username } [encrypt] | http { host | url } }**

no insert *xheader_field_name*

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

rule-variable

This command specifies the order of fields in the EDR. The following options were added to this command:

- http:
  - attribute-in-date
  - attribute-in-length
  - x-header

CLI (EDR Format Configuration Mode)

rule-variable *protocol rule* **priority** *priority*

no rule-variable *protocol rule* **[priority** *priority* **]**

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

rule-variable

This command specifies the order of fields in the UDR. The following option was added to this command:

- bearer:
  - serv-MDN

CLI (UDR Format Configuration Mode)

rule-variable *protocol rule* **priority** *priority*

no rule-variable *protocol rule* **[priority** *priority* **]**

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

eHRPD Commands - Modified in Release 10.0

This section provides information on HSGW commands modified in Release 10.0.

fqdn

You may now specify which P-GW you wish an HSGW interface to connect with by enabling topology matching within the FQDNs for both the HSGW service and P-GW service. Topology matching selects geographically closer nodes and reduces backhaul traffic for a specified interface.

The following optional keywords enable or disable topology matching when added to the beginning of an FQDN:

- **`topon.<`***`interface_name`***`>.`**

  Beginning an FQDN with **topon** initiates topology matching with available P-GWs in the network. Once this feature is enabled, the rest of the FQDN is processed from right to left until a matching regional designator is found on a corresponding P-GW FQDN.
- **`topoff.<`***`interface_name`***`>.`**

  By default, topology matching is disabled. If you enable topology matching for any interfaces within a node, however, all interfaces not using this feature should be designated with **topoff**.

CLI (HSGW Service Configuration Mode)

`[ default | no ] fqdn`

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

Firewall Commands - Modified in Release 10.0

This section provides information on commands modified for Release 10.0.

bearer

The following options have been deprecated from bearer and added within 3gpp:

- **apn**
- **imsi**

CLI (Firewall/Access Ruledef Configuration Mode)

[no] bearer 3gpp apn [case-sensitive] *operator value*

[no] bearer imsi { *operator msid* **| { !range | range } imsi-pool** *imsi_pool* **}**

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

firewall flow-recovery

This command configures Stateful Firewall and NAT Flow Recovery parameters. The optional keyword **no-flow-creation** was added to this command, this enables to specify not to create data session/flow-related information for downlink-initiated packets (from the Internet to the subscriber) while the firewall downlink flow-recovery timer is running, but send to subscriber.

CLI (Active Charging Service Configuration Mode)

firewall flow-recovery { downlink [[no-flow-creation] [timeout *timeout* **] +] | uplink [timeout** *timeout* **] }**

{ default | no } firewall flow-recovery { downlink | uplink }

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

GGSN Commands - Modified in Release 10.0

This section provides information on GGSN commands modified in Release 10.0.

gtpp storage-server local file

New keyword **force-file-rotation** added to force file rotation even if there are no CDRs at the specified time interval.

CLI (GTPP Server Group Configuration Mode)

gtpp storage-server local file {compression { gzip | none } | format { custom1 | custom2 | custom3 | custom4 | custom5 | custom6 | custom7 | custom8 } | name prefix *prefix* **| purge-processed-files [purge-interval** *purge_dur* **] | rotation { cdr-count** *count* **| time-interval** *time* **[force-file-rotation] | volume** *size***}}**

default gtpp storage-server local file {compression | format | name prefix | purge-processed-files | rotation { cdr-count | time-interval [force-file-rotation] | volume}}

no gtpp storage-server local file rotation { purge-processed-files | rotation { cdr-count | time-interval [force-file-rotation]} }

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

gtpu bind address

In the GTP-U Service Configuration Mode, the command **address** has been changed to **bind address** and support has been added for IPv6 addresses.

CLI (GTP-U Service Configuration Mode)

[no] bind { ipv4-address *address* **[ipv6-address** *address* **] | ipv6-address** *address* **[ipv4-address** *address* **] }**

HA Commands - Modified in Release 10.0

This section provides information on HA commands modified in Release 10.0.

None for this release.

HNB-GW Commands - Modified in Release 10.0

This section provides information on modified commands available in Release 10.0.

HNB-GW service is new in Release 10.0.

Several configuration mode and commands added/modified for this service.

NAT Commands - Modified in Release 10.0

This section provides information on NAT commands modified in Release 10.0.

bearer

The following options have been deprecated from bearer and added within 3gpp:

- **apn**
- **imsi**

CLI (Firewall/Access Ruledef Configuration Mode)

[no] bearer 3gpp apn [case-sensitive] *operator value*

[no] bearer imsi { *operator msid* **| { !range | range } imsi-pool** *imsi_pool* **}**

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

firewall nat-alg

This command enables/disables all/specified NAT Application Level Gateway (ALG). The following NAT ALG options were added to this command:

- **pptp**: Enables/disables Point-to-Point Tunneling Protocol (PPTP) NAT ALG processing.
- **sip**: Enables/disables Session Initiation Protocol (SIP) NAT ALG processing.

CLI (ACS Configuration Mode)

[default | no] firewall nat-alg { all | ftp | pptp | rtsp | sip }

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

firewall flow-recovery

This command configures Stateful Firewall and NAT Flow Recovery parameters. The optional keyword **no-flow-creation** was added to this command, this enables to specify not to create data session/flow-related information for downlink-initiated packets (from the Internet to the subscriber) while the firewall downlink flow-recovery timer is running, but send to subscriber.

CLI (Active Charging Service Configuration Mode)

firewall flow-recovery { downlink | uplink } [[no-flow-creation] [timeout *timeout* **] +]**

{ default | no } firewall flow-recovery { downlink | uplink }

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

idle-timeout

This command configures the maximum duration a flow can remain idle, in seconds, after which the system automatically terminates the flow. The alg-media keyword was added to this command. This enables configuring the Media Inactivity Timeout setting. The timeout value gets applied on the RTP and RTCP Media flows that are created for SIP/H.323 calls. The timeout value gets applied only on those flows that actually match the RTP and RTCP media pinholes that are created by the SIP/H.323 ALG.

CLI (ACS Configuration Mode)

idle-timeout { alg-media | icmp | tcp | udp } *idle_timeout_duration*

{ default | no } idle-timeout { alg-media | icmp | tcp | udp }

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

ip pool

This command enables to add/configure/delete IP address pools in a context. This command also enables to configure many-to-one and one-to-one NAT pools. The **group** keyword was added to the many-to-one and one-to-one NAT IP pool configuration options. This enables to bind discontigous IP address blocks in individual NAT IP pools with similar characteristics to a single NAT IP pool group.

CLI (Context Configuration Mode)

ip pool *pool_name* **{** *ip_address subnet_mask* **|** *ip_address_mask_combo* **| range** *start_ip_address end_ip_address* **} nat-one-to-one [alert-threshold [{ pool-free | pool-hold | pool-release | pool-used }** *low_thresh* **[clear** *high_thresh* **] +] [group-name** *group_name* **] [nat-binding-timer** *binding_timer* **] [nexthop-forwarding-address** *ip_address* **] [on-demand] [send-nat-binding-update] [srp-activate] +**

ip pool *pool_name* **{** *ip_address subnet_mask* **|** *ip_address_mask_combo* **| range** *start_ip_address end_ip_address* **} napt-users-per-ip-address** *users* **[alert-threshold [{ pool-free | pool-hold | pool-release | pool-used }** *low_thresh* **[clear** *high_thresh* **] +] [group-name** *group_name* **] [max-chunks-per-user** *chunks* **] [nat-binding-timer** *binding_timer* **] [nexthop-forwarding-address** *ip_address* **] [on-demand] [port-chunk-size** *size* **] [port-chunk-threshold** *chunk_threshold* **] [send-nat-binding-update] [srp-activate] +**

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

route priority

This command controls routing of packets to protocol analyzers. The following changes were made to this command:

- The optional keyword **advanced** was added to the **sip** keyword. This enables to route packets to the SIP ALG for processing. For SIP calls to work with NAT/Stateful Firewall, a SIP ALG is required to do payload translation of SIP packets and pin-hole (dynamic flow) creation for media packets. If the optional keyword **advanced** is configured, the packets matching the routing rule will be routed to SIP ALG for processing and not to the ECS SIP analyzer. If not configured, then packets will be routed to the ECS SIP analyzer for processing.
- The following protocol analyzer options were added to this command:
  - **pptp**: Enables to route traffic to the PPTP analyzer.
  - **tftp**: Enables to route traffic to the TFTP analyzer.

CLI (Rulebase Configuration Mode)

route priority *route_priority* **ruledef** *ruledef_name* **analyzer { dns | file-transfer | ftp-control | ftp-data | 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*

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

PDIF Commands - Modified in Release 10.0

This section provides information on PDIF commands modified in Release 10.0.

PDN Gateway Commands - Modified in Release 10.0

This section provides information on P-GW commands modified in Release 10.0.

gtpu bind address

In the GTP-U Service Configuration Mode, the command **address** has been changed to **bind address** and support has been added for IPv6 addresses.

CLI (GTP-U Service Configuration Mode)

[no] bind { ipv4-address *address* **[ipv6-address** *address* **] | ipv6-address** *address* **[ipv4-address** *address* **] }**

associate

In the P-GW Service Configuration Mode, the following changes were made to the **associate** command:

- The **accounting-policy** command was removed
- The **egtp-service** keyword now has an associated **lma-service** keyword to support eGTP to PMIP handovers.
- The **lma-service** keyword now has an associated **egtp-service** keyword to support PMIP to eGTP handovers.

CLI (P-GW Service Configuration Mode Commands

associate { egtp-service *name* **[lma-service** *name* **] | lma-service** *name* **[egtp-service** *name* **] | qci-qos-mapping** *name* **}**

authorize

In the P-GW Service Configuration Mode, the **authorize** command has been changed to **authorize-with-hss**.

The replaced command used the **external** keyword to indicate S6b connectivity to an external 3GPP AAA server. The old **internal** keyword specified that the system acquired subscriber authorization from an internal APN authorization configuration.

The new command simply toggles the command between the external S6b authorization (command enabled) and the internal APN authorization (command disabled).

CLI (P-GW Service Configuration Mode Commands

[default | no] authorize-with-hss

dns-pcscf context

In the P-GW Service Configuration Mode, the **dns-pcscf context** command has been changed to **dns-client context**.

Specifies the context to use where the DNS client resides to send DNS queries

CLI (P-GW Service Configuration Mode Commands

dns-client context *name*

[default | no] dns-client context

PDSN Commands - Modified for Release 10.0

This section provides information on PDSN commands modified in Release 10.0.

None for this release.

Peer-to-Peer - Modified for Release 10.0

This section provides information on Peer-to-Peer commands modified in Release 10.0.

P-GW Commands - Modified in Release 10.0

This section provides information on P-GW commands modified in Release 10.0.

fqdn

You may now specify which P-GW you wish an HSGW interface to connect with by enabling topology matching within the FQDNs for both the HSGW service and P-GW service. Topology matching selects geographically closer nodes and reduces backhaul traffic for a specified interface.

The following optional keywords enable or disable topology matching when added to the beginning of an FQDN:

- **topon.<***interface_name***>.**

  Beginning an FQDN with topon initiates topology matching with available HSGWs in the network. Once this feature is enabled, the rest of the FQDN is processed from right to left until a matching regional designator is found on a corresponding HSGW FQDN.

- **topoff.<***interface_name***>.**

  By default, topology matching is disabled. If you enable topology matching for any interfaces within a node, however, all interfaces not using this feature should be designated with topoff.

CLI (P-GW Service Configuration Mode)

fqdn host *domain_name* **realm** *realm_name*
[default | no] fqdn

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

Serving Gateway Commands - Modified in Release 10.0

This section provides information on S-GW commands modified in Release 10.0.

gtpu bind address

In the GTP-U Service Configuration Mode, the command **`address`** has been changed to **`bind address`** and support has been added for IPv6 addresses.

CLI (GTP-U Service Configuration Mode)

`[ no ] bind { ipv4-address` *`address`* **`[ ipv6-address`** *`address`* **`] | ipv6-address`** *`address`* **`[ ipv4-address`** *`address`* **`] }`**

Session Control Manager Commands - Modified for Release 10.0

The following commands have been modified in Release 10.0.

cscf ifc-spt-condition

Wildcard Extended Regular Expressions (ERE) are supported for **request-uri content** *uri_content*. For example, "sip.user[0-9]@192\\.168\\.176\\.150"

CLI (Context Configuration Mode)

cscf ifc-spt-condition name *cond_name* **{ request-uri content** *uri_content* **| session-case { originating-registered | originating-unregistered | terminating-registered | terminating-unregistered } | session-description** *sdp* **[content** *sdp_data* **] | sip-header** *hdr* **[content** *hdr_data* **] | sip-method** *method* **} [-noconfirm] [condition-negated]**

no cscf ifc-spt-condition name *cond_name*

exclude

Keyword **message** added to specify that MESSAGE SIP requests are to be excluded from Rf charging.

CLI (CSCF Charging Configuration Mode)

[no] exclude { custom *sip_method* **| invite | notify | register | subscribe | update | message }**

emergency-sessions

Configures the function to allow anonymous and/or non-emergency registered subscribers to initiate emergency sessions. The addition of 3GPP IM CN XML body in 380 response messages can also be allowed.

CLI (CSCF Proxy-CSCF Configuration Mode / CSCF Serving-CSCF Configuration Mode / CSCF SIP Proxy Configuration Mode)

emergency-sessions [3gpp-ims-xml-body | anonymous [3gpp-ims-xml-body] [non-emergency-registered] | non-emergency-registered [3gpp-ims-xml-body]]

[default | no] emergency-sessions

interrogating-cscf-role

All Interrogating-CSCF functions have been moved to the Serving-CSCF exclusively in v10.0 and beyond.

CLI (CSCF Proxy-CSCF Configuration Mode)

[no] interrogating-cscf-role

nat-policy

Policy type **bridge-network** added for S-CSCF bridging.

CLI (CSCF Service Configuration Mode)

nat-policy *policy_name* **{ private-address { address** *ip_address_mask* **| default | range** *start_ip_address end_ip_address* **} | bridge - network { address** *ip_address_mask* **| range** *start_ip_address end_ip_address* **} }**

no nat-policy *policy_name*

authentication

The S-CSCF now supports multiple authorization schemes, but this requires disabling all authorization configured in the S-CSCF service so that it will send “Unknown” in the Sip-Authorization-Scheme AVP. This allows the HSS to dictate authorization. The following commands disable all authorization configured in the S-CSCF service to allow HSS to control authorization:

authentication allow-noipauth

allow rfc3261-ua-interworking

no authentication aka-v1

no authentication md5

CLI (CSCF Serving-CSCF Configuration Mode / CSCF SIP Proxy Configuration Mode)

authentication { aka-v1 *value* **| allow-noauth [invite | re-register | register] | allow-noipauth [invite | re-register | register] | allow-unsecure | aor-auth | md5** *value* **}**

no authentication { aka-v1 | allow-noauth [invite | re-register | register] | allow-noipauth [invite | re-register | register] | allow-unsecure | aor-auth | md5 }

Obsoleted Commands

This section contains configuration commands that have been obsoleted in Release 10.0. Obsoleted commands in this version are divided into the following sections:

Common Commands - Obsoleted in Release 10.0

This section provides information on commands that are common to all products that were obsoleted in Release 10.0.

no quota request-trigger

The “no” variant of the **`quota request-trigger`** CLI command has been deprecated as the it contradicted with the “default” variant. If the entire keyword is typed out, the “no” variant will be accepted with a warning.

CLI (Credit Control Configuration Mode)

```
no quota request-trigger
```

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

Content Filtering Commands - Obsoleted in Release 10.0

This section provides information on CF commands that were obsoleted in Release 10.0.

None for this release.

ECS Commands - Obsoleted in Release 10.0

This section provides information on ECS commands that were obsoleted in Release 10.0.

priority

This CLI command has been deprecated as the precedence values of packet filters (those from Dynamic Rules, and those from Predefined Rules) are assigned by the PCEF based on an internal process. The CLI configurable precedences are not used internally.

CLI (ACS Packet Filter Configuration Mode)

priority *priority*

no priority

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

Firewall Commands - Obsoleted in Release 10.0

This section provides information on Firewall commands that were obsoleted in Release 10.0.

GGSN Commands - Obsoleted in Release 10.0

This section provides information on GGSN commands that were obsoleted in Release 10.0.

None for this release.

HA Commands - Obsoleted in Release 10.0

This section provides information on HA commands that were obsoleted in Release 10.0.

None for this release.

PDSN Commands - Obsoleted in Release 10.0

This section provides information on PDSN commands that were obsoleted in Release 10.0.

None for this release.

GTPP Storage Server (GSS)

This section provides information on GSS changes in Release 10.0.

GSS Changes in Release 10.0

This section provides information on GSS changes in Release 10.0.

None for this release.

Web Element Manager Changes

This section provides information on Web Element Manager changes in Release 10.0.

Support for the WEM Identifier Feature

WEM now provides a feature that enables the user to enter a unique WEM Identifier text string upon login that will appear at the top of every WEM screen opened during a user session. This text will be prepended to the existing text on the Title Bar. The WEM Identifier text can be used to differentiate between multiple WEM sessions opened by individual users.

This feature allows users to differentiate between multiple WEM sessions opened by a single user.

WEM system administrators will be required to modify two files in the *ems\client* directory to enable this feature.

Web Element Manager Path

WEM Overview\Using WEM\Enabling the WEM Identifier

Enhancement to getSupportDetails.pl

The WEM getSupportDetails.pl script has been enhanced to allow the user to specify the output directory for the emssupportDetails.tar.gz file if the output directory is different from the default output directory (/tmp/). This script collects different log files and captures the output of certain system commands that aid in troubleshooting issues. This script is packaged with the WEM Server in the <EMS_INSTALL_DIR>/tools/supportdetails/ directory.

Web Element Manager Path

WEM Installation and Administration Guide\Chapter 4, WEM Server Files and Operation\Capturing WEM Server Logs using Script

Windows 7 Support for WEM

WEM now can be accessed by client machines running the Windows 7 operating system.

Web Element Manager Path

- WEM Installation and Administration Guide\Chapter 1, Web Element Manager Overview\Client Access
- WEM Installation and Administration Guide\Chapter 8, Preparing and Using the Client Workstation\Placement of Required Files

Enhancement to WEM Server nms.cfg File

The WEM Server *nms.cfg* file has been enhanced to allocate an additional ServerIIOPPort for ASR 5000 to WEM server callback information.

Using this port, three sequential upward ports (15000, 15001 and 15002) will be used to create POAs. If this value is changed, the SERVER_BASE_PORT parameter in both the ems/client/img.html and ems/client/imgdebug.html files must also be changed.

Web Element Manager Path

<WEM INSTALL DIR>/server/etc

Support for CSCF Parameters in Subscriber Configuration

WEM now supports the adding, modifying and viewing of Call Session Control Function (CSCF) parameters for subscriber configuration.

Web Element Manager Path

- Configuration\Context Provisioning\Subscriber\Add\CSCF Tab
- Configuration\Context Provisioning\Subscriber\Modify\CSCF Tab
- Configuration\Context Provisioning\Subscriber\Details\CSCF Tab

CHAPTER 4
ACCOUNTING MANAGEMENT

This section contains additions and changes made to the accounting-related parameters available in Release 10.0. Topics covered in this chapter are:

Bulk Statistic Enhancements in Release 10.0

This section lists bulk statistic additions and changes in Release 10.0. Detailed information on bulk statistics is located in both the *System Administration Guide* and in the *Statistics and Counters Reference*. Bulk statistic changes in this version are divided into the following sections:

New Bulk Statistics

Support for the following bulk statistics were added in Release 10.0.

CSCF Schema

- emerg-priv-calls
- msrp-sent
- msrp-recv
- fhloerrrx
- fhloerrtx
- calldur-lt-01sec
- calldur-01to10sec
- calldur-10to30sec
- calldur-30to60sec
- calldur-60to90sec
- calldur-90to120sec
- calldur-120to150sec
- calldur-150to180sec
- calldur-03to04min
- calldur-04to05min
- calldur-05to06min
- calldur-06to07min
- calldur-07to08min
- calldur-08to09min
- calldur-09to11min
- calldur-11to13min
- calldur-13to15min
- calldur-15to17min
- calldur-17to19min
- calldur-19to21min
- calldur-21to23min

- calldur-23to25min
- calldur-25to27min
- calldur-27to29min
- calldur-29to60min
- calldur-gt-60min

ECS Schema

- p2p-freenet-uplnk-bytes
- p2p-freenet-dwlnk-bytes
- p2p-freenet-uplnk-pkts
- p2p-freenet-dwlnk-pkts
- p2p-aimini-uplnk-bytes
- p2p-aimini-dwlnk-bytes
- p2p-aimini-uplnk-pkts
- p2p-aimini-dwlnk-pkts
- p2p-battlefld-uplnk-bytes
- p2p-battlefld-dwlnk-bytes
- p2p-battlefld-uplnk-pkts
- p2p-battlefld-dwlnk-pkts
- p2p-openft-uplnk-bytes
- p2p-openft-dwlnk-bytes
- p2p-openft-uplnk-pkts
- p2p-openft-dwlnk-pkts
- p2p-qqgame-uplnk-bytes
- p2p-qqgame-dwlnk-bytes
- p2p-qqgame-uplnk-pkts
- p2p-qqgame-dwlnk-pkts
- p2p-quake-uplnk-bytes
- p2p-quake-dwlnk-bytes
- p2p-quake-uplnk-pkts
- p2p-quake-dwlnk-pkts
- p2p-secondlife-uplnk-bytes
- p2p-secondlife-dwlnk-bytes
- p2p-secondlife-uplnk-pkts
- p2p-secondlife-dwlnk-pkts
- p2p-actsync-uplnk-bytes
- p2p-actsync-dwlnk-bytes
- p2p-actsync-uplnk-pkts
- p2p-actsync-dwlnk-pkts

- p2p-nimbuzz-uplnk-bytes
- p2p-nimbuzz-dwlnk-bytes
- p2p-nimbuzz-uplnk-pkts
- p2p-nimbuzz-dwlnk-pkts
- p2p-iax-uplnk-bytes
- p2p-iax-dwlnk-bytes
- p2p-iax-uplnk-pkts
- p2p-iax-dwlnk-pkts
- p2p-paltalk-uplnk-bytes
- p2p-paltalk-dwlnk-bytes
- p2p-paltalk-uplnk-pkts
- p2p-paltalk-dwlnk-pkts
- p2p-warcft3-uplnk-bytes
- p2p-warcft3-dwlnk-bytes
- p2p-warcft3-uplnk-pkts
- p2p-warcft3-dwlnk-pkts
- p2p-rdp-uplnk-bytes
- p2p-rdp-dwlnk-bytes
- p2p-rdp-uplnk-pkts
- p2p-rdp-dwlnk-pkts
- p2p-iptv-uplnk-bytes
- p2p-iptv-dwlnk-bytes
- p2p-iptv-uplnk-pkts
- p2p-iptv-dwlnk-pkts
- p2p-pandora-uplnk-bytes
- p2p-pandora-dwlnk-bytes
- p2p-pandora-uplnk-pkts
- p2p-pandora-dwlnk-pkts

Diameter Accounting Schema

- vpnid
- vpnname
- ipaddr
- port
- servertype
- group
- req-sent
- req-retried
- rsp-rcvd

- req-timeout
- rsp-bad-resp
- rsp-malformed
- rsp-dropped
- start-sent
- stop-sent
- interim-sent
- start-retries
- stop-retries
- interim-retries

Diameter Authentication Schema

- vpnid
- vpnname
- ipaddr
- port
- servertype
- group
- der-req-id-sent
- der-req-aka-chal-sent
- der-req-retried
- dea-chal-rcvd
- dea-acpt-rcvd
- dea-timeout
- dea-badauth
- dea-malformed
- dea-malformed-avp
- dea-dropped
- rar-req-rcvd
- raa-ans-accpt-sent
- aar-req-sent
- str-req-sent
- str-req-retried
- sta-ans-accpt-rcvd
- asr-req-rcvd
- asa-rsp-accpt-sent
- asa-rsp-rej-sent
- req-sock-write-err
- rsp-sock-write-err

- any-sock-read-err
- rem-disconnect
- loc-disconnect

IMSA Schema

- dpca-fail-connfh-totmsgtmo
- dpca-fail-connfh-totmsgsenderr
- dpca-fail-rescodefh-confrescode
- dpca-fail-rescodefh-unhunkrescode

NAT Realm Schema

- nat-rlm-port-chunk-size
- nat-rlm-port-chunk-average-usage-tcp
- nat-rlm-port-chunk-average-usage-udp
- nat-rlm-port-chunk-average-usage-others
- nat-rlm-max-port-chunk-subs
- nat-rlm-max-port-chunk-used
- nat-rlm-max-cur-port-chunk-subs
- nat-rlm-max-cur-port-chunk-used

Modified Bulk Statistics

The following bulk statistics were modified in Release 10.0.

P-GW Node Level Schema

The following statistics were added to this schema:

- sessstat-bearact-def
- sessstat-bearact-ue-init-ded
- sessstat-bearact-nw-init-ded
- sessstat-bearrel-nwdedadmin
- sessstat-bearrel-nwdedgtp
- sessstat-bearrel-nwdedmme
- sessstat-bearrel-nwdeddefbear
- sessstat-bearrel-nwdedgxdisc
- sessstat-bearrej-uereq-nores
- sessstat-bearrej-nwreq-nores
- sessstat-bearrej-nwreq-nomem
- sessstat-bearrej-nwreq-sysfail
- sessstat-bearmodfail-ueinit
- sessstat-bearmodfail-nwinit
- sessstat-bearmodfail-nwnores

- sessstat-bearmodfail-nwnomem
- sessstat-bearmodfail-nwsysfail
- sessstat-bearmodfail-nwsemtft
- sessstat-bearmodfail-nwsyntft
- sessstat-bearmodfail-nwsempkt
- sessstat-bearmodfail-nwsynpkt
- sessstat-bearrel-nwdefadmin
- sessstat-bearrel-nwdefgtp
- sessstat-bearrel-nwdefsgw
- sessstat-bearrel-nwdefmme
- sessstat-bearrel-nwdedadmin
- sessstat-bearrel-nwdedgtp
- sessstat-bearrel-nwdedmme
- sessstat-bearrel-nwdeddefbear
- sessstat-bearrel-nwdedgxdisc
- subdatastat-uppktfwd-stdqcinongbr
- subdatastat-uppktfwd-stdqcigbr
- subdatastat-uppktfwd-totgbr
- subdatastat-uppktfwd-totnongbr
- subdatastat-upbytefwd-stdqcinongbr
- subdatastat-upbytefwd-stdqcigbr
- subdatastat-upbytefwd-totgbr
- subdatastat-upbytefwd-totnongbr
- subdatastat-downpktfwd-stdqcinongbr
- subdatastat-downpktfwd-stdqcigbr
- subdatastat-downpktfwd-totgbr
- subdatastat-downpktfwd-totnongbr
- subdatastat-downbytefwd-stdqcinongbr
- subdatastat-downbytefwd-stdqcigbr
- subdatastat-downbytefwd-totgbr
- subdatastat-downbytefwd-totnongbr
- subdatastat-uppktdrop-stdqcinongbr
- subdatastat-uppktdrop-stdqcigbr
- subdatastat-uppktdrop-totgbr
- subdatastat-uppktdrop-totnongbr
- subdatastat-upbytedrop-stdqcinongbr
- subdatastat-upbytedrop- stdqcigbr
- subdatastat-upbytedrop-totgbr

- subdatastat-upbytedrop-totnongbr
- subdatastat-downpktdrop-stdqcinongbr
- subdatastat-downpktdrop-stdqcigbr
- subdatastat-downpktdrop-totgbr
- subdatastat-downpktdrop-totnongbr
- subdatastat-downbytedrop-stdqcinongbr
- subdatastat-downbytedrop-stdqcigbr
- subdatastat-downbytedrop-totgbr
- subdatastat-downbytedrop-totnongbr
- subdatastat-totuppktdropmbrexc
- subdatastat-uppktdropmbrexc-qci1
- subdatastat-uppktdropmbrexc-qci2
- subdatastat-uppktdropmbrexc-qci3
- subdatastat-uppktdropmbrexc-qci4
- subdatastat-uppktdropmbrexc-qci5
- subdatastat-uppktdropmbrexc-qci6
- subdatastat-uppktdropmbrexc-qci7
- subdatastat-uppktdropmbrexc-qci8
- subdatastat-uppktdropmbrexc-qci9
- subdatastat-uppktdropmbrexc-stdqcinongbr
- subdatastat-uppktdropmbrexc-stdqcigbr
- subdatastat-uppktdropmbrexc-qcinongbr
- subdatastat-uppktdropmbrexc-qcigbr
- subdatastat-uppktdropmbrexc-totgbr
- subdatastat-uppktdropmbrexc-totnongbr
- subdatastat-totupbytedropmbrexc
- subdatastat-upbytedropmbrexc-qci1
- subdatastat-upbytedropmbrexc-qci2
- subdatastat-upbytedropmbrexc-qci3
- subdatastat-upbytedropmbrexc-qci4
- subdatastat-upbytedropmbrexc-qci5
- subdatastat-upbytedropmbrexc-qci6
- subdatastat-upbytedropmbrexc-qci7
- subdatastat-upbytedropmbrexc-qci8
- subdatastat-upbytedropmbrexc-qci9
- subdatastat-upbytedropmbrexc-stdqcinongbr
- subdatastat-upbytedropmbrexc-stdqcigbr
- subdatastat-upbytedropmbrexc-qcinongbr

- subdatastat-upbytedropmbrexc-qcigbr
- subdatastat-upbytedropmbrexc-totgbr
- subdatastat-upbytedropmbrexc-totnongbr

S-GW Node Level Schema Statistics

The following statistics were added to this schema:

- sessstat-pdnrelrsn-pathfail-S11
- sessstat-pdnrelrsn-pathfail-S5
- sessstat-pdnrelrsn-pathfail-S5-u
- sessstat-pdnrelrsn-pathfail-S1-u
- sessstat-pdnrejrsn-license
- sessstat-pdnrejrsn-newcall-policy
- sessstat-pdnrejrsn-overload
- sessstat-pdnrejrsn-cong

Obsoleted Bulk Statistics

The following bulk statistics were obsoleted in Release 10.0.

None for this release.

Web Element Manager Path

Click Accounting | Bulk Statistics Configuration.

CDR Enhancements

This section lists new custom GTPP dictionaries in Release 10.0. Refer to the *AAA Interface Configuration and Reference* for details.

Command Enhancements

None for this release.

New Commands

None for this release.

RADIUS Attributes in Release 10.0

This section lists additions and changes to RADIUS AVPs in Release 10.0. Refer to the *AAA Interface Configuration and Reference* for details.

New Attributes

The following RADIUS attributes are new in Release 10.0.

- 3GPP2-IP-Services-Authorized
- 3GPP2-DNS-Server-IPV6-Addr
- SN-TrafficSelector-Class
- SN1-NAT-IP-Address-Old
- WiMAX-Prepaid-Tariff-Switch

Modified Attributes

The following RADIUS attributes were modified in Release 10.0.

- 3GPP2-IP-QOS
- 3GPP2-Service-Option
- Protocol
- SN-Disconnect-Reason
- SN1-Disconnect-Reason
- Transmission-Policy
- WiMAX-Capability
- WiMAX-NSP-ID
- WiMAX-Packet-Flow-Descriptor
- WiMAX-QoS-Descriptor

Removed Attributes

None for this release.

Diameter Attributes in Release 10.0

This section lists additions and changes to Diameter attributes in Release 10.0. Refer to the *AAA Interface Reference* for details.

New Attributes

The following Diameter attributes are new in Release 10.0:

- 3GPP-WLAN-APN-Id
- Associated-Registered-Identities
- Call-ID-SIP-Header
- Charging-Characteristics
- Charging-Data
- Contact
- From-SIP-Header
- GMLC-Number
- Loose-Route-Indication
- Multiple-Registration-Indication
- Path
- Record-Route
- Restoration-Info
- SCSCF-Restoration-Info
- Session-Priority
- Session-Request-Type
- SGSN-Number
- SN-Phase0-PSAPName
- Subscription-Info
- To-SIP-Header
- Usage-Monitoring-Information
- Usage-Monitoring-Level
- Usage-Monitoring-Report
- Usage-Monitoring-Support
- Wildcarded-IMPU

Modified Attributes

The following Diameter attributes were modified in Release 10.0:

- Event-Trigger
- SIP-Auth-Data-Item
- SN-Service-Flow-Detection

Removed Attributes

The following Diameter attributes were removed in Release 10.0:

None for this release.

Web Element Manager Enhancements

This section describes the Accounting enhancements that were made for Web Element Manager release 10.0.

Bulk Statistics Enhancements

EGPTC Bulk Statistics

The following EGTPC Bulks Statistics were added in release 10.0.

Table 4-1 EGTPC Bulk Statistics Added in WEM Release 10.0

Statistic Category	Name
Create Ind Data Forwarding Tunnel Request	■ tun-sent-creinddatafwdngreq ■ tun-sent-retranscreinddatafwdngreq ■ tun-recv-creinddatafwdngreq ■ tun-recv-retranscreinddatafwdngreq
Create Ind Data Forwarding Tunnel Response	■ tun-sent-creinddatafwdngrsp ■ tun-sent-creinddatafwdngrspaccept ■ tun-sent-creinddatafwdngrspdenied ■ tun-sent-retranscreinddatafwdngrsp ■ tun-recv-creinddatafwdngrsp ■ tun-recv-creinddatafwdngrspdenied
Delete Ind Data Forwarding Tunnel Request	■ tun-sent-delinddatafwdngreq ■ tun-sent-retransdelinddatafwdngreq ■ tun-recv-delinddatafwdngreq ■ tun-recv-retransdelinddatafwdngreq
Delete Ind Data Forwarding Tunnel Response	■ tun-sent-delinddatafwdngrsp ■ tun-sent-delinddatafwdngrspaccept ■ tun-sent-delinddatafwdngrspdenied ■ tun-recv-delinddatafwdngrsp ■ tun-recv-delinddatafwdngrspaccept ■ tun-recv-delinddatafwdngrspdenied

Web Element Manager Path:

Accounting\View/Graph Bulk Statistics\Dialog Boxes\Counter Categories & Analysis Counters List

MAG Bulk Statistics

The following MAG Bulk Statistics were added for release 10.0.

Table 4-2 MAG Bulk Statistics Added in WEM Release 10.0

Statistic Category	Name
Denied by LMA	■ deniedlma-grekey
Sent Revocation Trigger Reasons	■ rcvdbindrevtrig-reserved ■ rcvdbindrevtrig-unspecified ■ rcvdbindrevtrig-admin ■ rcvdbindrevtrig-maghoffsameatt ■ rcvdbindrevtrig-maghoff-unknown ■ rcvdbindrevtrig-maghoff-diffatt ■ rcvdbindrevtrig-perpeer ■ rcvdbindrevtrig-nodelocal ■ rcvdbindrevtrig-userinitsess ■ rcvdbindrevtrig-accessnwsess ■ rcvdbindrevtrig-ipv4hoabind ■ rcvdbindrevtrig-syncbce ■ rcvdbindrevtrig-unknown
Sent Revocation ACK Status	■ sentrevack-success ■ sentrevack-partialsuccess ■ sentrevack-nobinding ■ sentrevack-noipv4hoabind ■ sentrevack-revocnotauth ■ sentrevack-bindingnotidentified ■ sentrevack-revocfailmnattch ■ sentrevack-unknown

Web Element Manager Path

Accounting\View/Graph Bulk Statistics\Dialog Boxes\Counter Categories & Analysis Counters List

MME Bulk Statistics

The following MME Bulk Statistics were added for release 10.0.

Table 4-3 MME Bulk Statistics Added in WEM Release 10.0

Statistic Category	Sub-Category	Name
EMM Events	Associations by Attach using IMSI	■ emmevent-associmsi-attempt ■ emmevent-associmsi-success ■ emmevent-associmsi-failure
	Associations by Attach using Local GUTI	■ emmevent-assoclocguti-attempt ■ emmevent-assoclocguti-success ■ emmevent-assoclocguti-failure
	Associations by Attach using Non-local GUTI	■ emmevent-assocnonlocguti-attempt ■ emmevent-assocnonlocguti-success ■ emmevent-assocnonlocguti-failure
	Detaches UE Initiated	■ emmevent-detachhssinit-attempt ■ emmevent-detachhssinit-success ■ emmevent-detachhssinit-failure
	Detaches NW Initiated	■ emmevent-detachnwinit-attempt ■ emmevent-detachnwinit-success ■ emmevent-detachnwinit-failure

Web Element Manager Path:

Accounting\View/Graph Bulk Statistics\Dialog Boxes\Counter Categories & Analysis Counters List

PGW Bulk Statistics

The following PGW bulk statistics were added for release 10.0.

Table 4-4 PGW Bulk Statistics Added in WEM Release 10.0

Statistic Category	Sub-Category	Name
UE-Initiated Mod Fail	QOS Changed	■ sessstat-bearmodfail-qos-uenores ■ sessstat-bearmodfail-qos-uesemtft ■ sessstat-bearmodfail-qos-uesyntft ■ sessstat-bearmodfail-qos-uesempkt ■ sessstat-bearmodfail-qos-uesynpkt
PGW Statistics	No QOS Changed	■ sessstat-bearmodfail-qos-nwnores ■ sessstat-bearmodfail-qos-nwnomem ■ sessstat-bearmodfail-qos-nwsysfail ■ sessstat-bearmodfail-qos-nwsemtft ■ sessstat-bearmodfail-qos-nwsyntft ■ sessstat-bearmodfail-qos-nwsempkt ■ sessstat-bearmodfail-qos-nwsynpkt
	Intra Technology Handover - Inter SGSN Handover	■ handoverstat-intersgsnatt ■ handoverstat-intersgsnsucc ■ handoverstat-intersgsnfail
	Intra Technology Handover - Inter SGW Handover	■ handoverstat-intersgwatt ■ handoverstat-intersgwsucc ■ handoverstat-intersgwfail
	Intra Technology Handover - Inter HSGW Handover	■ handoverstat-interhsgwatt ■ handoverstat-interhsgwsucc ■ handoverstat-interhsgwfail
	Inter Technology Handover - GNGP-to-LTE	■ handoverstat-gngptolteatt ■ handoverstat-gngptoltesucc ■ handoverstat-gngptoltefail
	Inter Technology Handover - LTE-to-GNGP	■ handoverstat-ltetogngpatt ■ handoverstat-ltetogngpsucc ■ handoverstat-ltetogngpfail
	Inter Technology Handover - LTE-to-eHRPD	■ handoverstat-ltetoehrpdatt ■ handoverstat-ltetoehrpdsucc ■ handoverstat-ltetoehrpdfail
	Inter Technology Handover - eHRPD-to-LTE	■ handoverstat-ehrpdtolteatt ■ handoverstat-ehrpdtoltesucc ■ handoverstat-ehrpdtoltefail

Web Element Manager Path

Accounting\View/Graph Bulk Statistics\Dialog Boxes\Counter Categories & Analysis Counters List

IMSA Bulk Statistics

The following IMSA bulk statistics were added for release 10.0.

Table 4-5 PGW Bulk Statistics Added in WEM Release 10.0

Statistic Category	Sub-Category	Description
IMSA Statistics	DPCA Failure Handling Stats - Connection Based FH	■ dpca-fail-connfh-totmsgtmo ■ dpca-fail-connfh-totmsgsenderr
	Total Message Timeouts	■ dpca-ccai-timeout ■ dpca-ccat-timeout ■ dpca-ccau-timeout
	Total Message Send Errors	■ dpca-ccri-send-error ■ dpca-ccru-send-error ■ dpca-ccrt-send-error
	Result Code Based FH	■ dpca-fail-rescodefh-confrescode ■ dpca-fail-rescodefh-unhunkrescode

Web Element Manager Path

Accounting\View/Graph Bulk Statistics\Dialog Boxes\Counter Categories & Analysis Counters List

LMA Bulk Statistics

The following LMA bulk statistics were added for release 10.0.

Table 4-6 LMA Bulk Statistics Added in WEM Release 10.0

Statistic Category	Description
Binding Update Deny Reasons	■ bindupd-denygrekey
Binding Update Discard Reasons	■ bindupd-discardrevoc

Web Element Manager Path:

Accounting\View/Graph Bulk Statistics\Dialog Boxes\Counter Categories & Analysis Counters List

BCMCS Bulk Statistics

The following BCMCS bulk statistics were added for release 10.0.

Table 4-7 BCMCS Bulk Statistics Added in WEM Release 10.0

Statistic Category	Description
BCMCS Service Request/Response	■ srsp-recv-total ■ srsp-accept-total ■ srsp-denied-total ■ srsp-discard-total ■ srsp-accept-initial ■ srsp-recv-initial ■ srsp-denied-initial ■ srsp-discard-initial ■ srsp-accept-renew ■ srsp-denied-renew ■ srsp-recv-renew ■ srsp-discard-renew ■ srsp-send-error
BCMCS Service Request Denied	■ srsp-deny-unspec ■ srsp-deny-auth ■ srsp-deny-idmismatch ■ srsp-deny-unknownbsn
BCMCS SRQ Denied - Insufficient Resource Reasons	■ srsp-deny-noresource-nosessmgr ■ srsp-deny-noresource-nomem ■ srsp-deny-noresource-sessmgrretrie ■ srsp-deny-noresource-inputq
BCMCS SRQ Denied - Poorly Formed Request Reasons	■ srsp-deny-badrequest-alrdorm ■ srsp-deny-badrequest-alractive ■ srsp-deny-badrequest-other
BCMCS SRQ Denied - Overload/ Congestion Control	■ srsp-deny-cong-adminprohib ■ srsp-deny-cong-unknownbsn

Table 4-7 BCMCS Bulk Statistics Added in WEM Release 10.0

Statistic Category	Description
BCMCS Registration Request/Reply	■ recv-total ■ accept-tota ■ denied-total ■ discard-total ■ accept-initial ■ recv-initial ■ denied-initial ■ discard-initial ■ accept-renew ■ denied-renew ■ discard-renew ■ recv-renew ■ active-start-renew ■ active-stop-renew ■ accept-dereg ■ denied-dereg ■ discard-dereg ■ recv-dereg ■ active-stop-dereg ■ send-error
BCMCS Registration Request Denied	■ deny-unspec ■ deny-adminprohib ■ deny-noresource ■ deny-auth ■ deny-idmismatch ■ deny-badrequest ■ deny-unknownbsn ■ deny-revtununavail ■ deny-revtunreq ■ deny-unrecogvend ■ deny-sessclosed ■ deny-bsninfo
BCMCS RRQ Denied - Insufficient Resource Reasons	■ deny-noresource-nomem ■ deny-noresource-sessmgrretried ■ deny-noresource-inputq
BCMCS RRQ Denied - Poorly Formed Request Reasons	■ deny-badrequest-alrdorm ■ deny-badrequest-alractive ■ deny-badrequest-other
BCMCS RRQ Denied - Overload/Congestion Contro	■ deny-cong-adminprohib ■ deny-cong-unknownbsn

Table 4-7 BCMCS Bulk Statistics Added in WEM Release 10.0

Statistic Category	Description
BCMCS Registration Update/Ack	■ upd-total ■ upd-accept ■ upd-denied ■ upd-unack ■ upd-trans ■ upd-retrans ■ upd-received ■ upd-ack-received ■ upd-discard ■ upd-senderror
BCMCS Registration Update Send Reason	■ upd-lifetime ■ upd-uplyrinit ■ upd-other ■ upd-smgrexit
BCMCS Registration Update Denied	■ upddeny-unspec ■ upddeny-adminprohib ■ upddeny-auth ■ upddeny-idmismatch ■ upddeny-badrequest
Security Violations	■ sec-violations ■ sec-badauth ■ sec-badid ■ sec-badspi ■ sec-mnhaauth ■ sec-regupdate
BCMCS Registration Ack Discard Reasons	■ disc-absent ■ disc-nomem ■ disc-malform ■ disc-authfail ■ disc-bounce ■ disc-inputq ■ disc-mismatchid ■ disc-invpktlen ■ disc-misc

Web Element Manager Path

Accounting\View/Graph Bulk Statistics\Dialog Boxes\Counter Categories & Analysis Counters List

DIAMETER Bulk Statistics

The following DIAMETER bulk statistics were added for release 10.0.

Table 4-8 DIAMETER Bulk Statistics Added in WEM Release 10.0

Statistic Category	Description
Diameter Auth	■ der-req-id-sent ■ der-req-aka-chal-sent ■ der-req-retried ■ dea-chal-rcvd ■ dea-acpt-rcvd ■ dea-timeout ■ dea-badauth ■ dea-malformed ■ dea-malformed-avp ■ dea-dropped ■ rar-req-rcvd ■ raa-ans-accpt-sent ■ aar-req-sent ■ str-req-sent ■ str-req-retried ■ sta-ans-accpt-rcvd ■ asr-req-rcvd ■ asa-rsp-accpt-sent
Diameter Acct	■ req-sent ■ req-retried ■ rsp-rcvd ■ req-timeout ■ rsp-bad-resp ■ rsp-malformed ■ rsp-dropped ■ start-sent ■ stop-sent ■ interim-sent ■ start-retries ■ stop-retries ■ interim-retries

Web Element Manager Path

Accounting\View/Graph Bulk Statistics\Dialog Boxes\Counter Categories & Analysis Counters List

DCCA Bulk Statistics

The following DCCA bulk statistics were added for release 10.0.

Table 4-9 DCCA Bulk Statistics Added in WEM Release 10.0

Statistic Category	Description
DCCA Statistics	■ ccr-inisent ■ ccr-initimeout ■ ccr-updsent ■ ccr-tersent ■ cca-updrec ■ cca-inirec ■ cca-updtimeout ■ cca-terrec ■ cca-tertimeout ■ reauth-anssent ■ reauth-reqrec

Web Element Manager Path:

Accounting\View/Graph Bulk Statistics\Dialog Boxes\Counter Categories & Analysis Counters List

DPCA Bulk Statistics

The following DPCA bulk statistics were added for release 10.0.

Table 4-10 DPCA Bulk Statistics Added in WEM Release 10.0

Statistic Category	Description
DPCA Statistics	■ ccr-inisent ■ cca-inirec ■ ccr-initimeout ■ ccr-updsent ■ cca-updrec ■ ccr-updtimeout ■ ccr-tersent ■ cca-terrec ■ ccr-tertimeout ■ reauth-anssent ■ reauth-reqrec

Web Element Manager Path

Accounting\View/Graph Bulk Statistics\Dialog Boxes\Counter Categories & Analysis Counters List

NAT Realm Bulk Statistics

The following NAT Realm bulk statistics were added for release 10.0.

Table 4-11 NAT Realm Bulk Statistics Added in WEM Release 10.0

Statistic Category	Name
NAT Realm Statistics	■ nat-rlm-port-chunk-average-usage-tcp ■ nat-rlm-port-chunk-average-usage-udp ■ nat-rlm-port-chunk-average-usage-others ■ nat-rlm-max-port-chunk-used ■ nat-rlm-max-cur-port-chunk-used ■ nat-rlm-max-cur-port-chunk-subs ■ nat-rlm-max-port-chunk-subs

Web Element Manager Path

Accounting\View/Graph Bulk Statistics\Dialog Boxes\Counter Categories & Analysis Counters List

ECS Bulk Statistics

The following ECS bulk statistics were added for release 10.0.

Table 4-12 ECS Bulk Statistics Added in WEM Release 10.0

Statistic Category	Sub-Category	Name
ECS Statistics	ACF	■ acf-req-created ■ acf-wr-req-succ ■ acf-wr-req-failed ■ acf-rd-rsp-succ ■ acf-rd-rsp-failed ■ acf-http-permit ■ acf-http-deny ■ acf-http-redirect ■ acf-wap-permit ■ acf-wap-deny ■ acf-wap-redirect ■ dns-req-aaaa-query ■ dns-rsp-aaaa-query
	Historical Statistics	■ ecs-ppruleshit

Web Element Manager Path

Accounting\View/Graph Bulk Statistics\Dialog Boxes\Counter Categories & Analysis Counters List

GTPC Bulk Statistics

The following GTPC bulk statistics were added for release 10.0.

Table 4-13 GTPC Bulk Statistics Added in WEM Release 10.0

Statistic Category	Sub-Category	Description
GTPC Statistics	PDU Notification Reject	■ num-dt-established ■ num-dt-torn-by-sgsn ■ num-dt-recv-err-ind
	Update PDP Context	■ upc-tx-dt-upd
	Preservation Mode Stats	■ sess-in-lorc ■ transition-to-lorc
	PDU Notification	■ pdu-notif-accpet

Web Element Manager Path

Accounting\View/Graph Bulk Statistics\Dialog Boxes\Counter Categories & Analysis Counters List

SGTP Statistics

The following SGTP bulk statistics were added for release 10.0.

Table 4-14 SGTP Bulk Statistics Added in WEM Release 10.0

Category	Sub-Category	Description
SGTP Statistics	Tunnel Management Messages	■ sgtpc-total-pdu-not-req ■ sgtpc-pdu-not-req-v1-pri ■ sgtpc-pdu-not-req-v0-pri ■ sgtpc-pdu-not-req-sec ■ sgtpc-pdu-not-req-v1-pri-ret ■ sgtpc-pdu-not-req-v0-pri-ret ■ sgtpc-pdu-not-req-sec-ret ■ sgtpc-pdu-not-req-accept-v1 ■ sgtpc-pdu-not-req-accept-v0 ■ sgtpc-pdu_not-req-denied ■ sgtpc-total-pdu-not-rej-req ■ sgtpc-pdu-not-rej-req-v1-pri ■ sgtpc-pdu-not-rej-req-v0-pri ■ sgtpc-pdu-not-rej-req-v1-pri-ret ■ sgtpc-pdu-not-rej-req-v0-pri-ret ■ sgtpc-pdu-not-rej-req-accept-v1 ■ sgtpc-pdu-not-rej-req-accept-v0
	Location Management Messages	■ sgtpc-total-sri-req ■ sgtpc-sri-req-v1 ■ sgtpc-sri-req-v0 ■ sgtpc-sri-req-v1-ret ■ sgtpc-sri-req-v0-ret ■ sgtpc-fail-rpt-req-v1 ■ sgtpc-fail-rpt-req-v0 ■ sgtpc-fail-rpt-req-v1-ret ■ sgtpc-fail-rpt-req-v0-ret

Web Element Manager Path

Accounting\View/Graph Bulk Statistics\Dialog Boxes\Counter Categories & Analysis Counters List

GPRS Statistics

The following GPRS Statistics were added for release 10.0.

Table 4-15 GPRS Bulk Statistics Added in WEM Release 10.0

Statistic Category	Sub-Category	Description
GPRS Statistics	BSSGP Statistics	■ bssgp-pkt-drop-flowctrl-queue-full ■ bssgp-downlink-pktdrop

Web Element Manager Path

Accounting\View/Graph Bulk Statistics\Dialog Boxes\Counter Categories & Analysis Counters List

SGSN Bulk Statistics

The following SGSN bulk statistics were added for release 10.0.

Table 4-16 SGSN Bulk Statistics Added in WEM Release 10.0

Category	Sub-Category	Description
SGSN Statistics	Session Statistics	■ 3G-network-sharing-supp-ue ■ 3G-network-sharing-non-supp-ue ■ 2G-total-attach-req ■ 3G-ret-imsi-attach ■ 2G-ret-imsi-attach
	Message Statistics - Specific Procedures	■ 2G-total-attach-req ■ 3G-ret-imsi-attach ■ 3G-ret-attach-accept ■ 2G-ret-attch-accept ■ 3G-total-attach-fail-all ■ 2G-total-attach-fail-all ■ 3G-ret-intra-rau ■ 2G-ret-intra-rau ■ 3G-ret-periodic-rau ■ 2G-ret-periodic-rau ■ 3G-ret-inter-sgsn-rau ■ 2G-ret-inter-sgsn-rau ■ 3G-ret-rau-accept-intra ■ 2G-ret-rau-accept-intra ■ 3G-ret-rau-accept-inter ■ 2G-ret-rau-accept-inter

Table 4-16 SGSN Bulk Statistics Added in WEM Release 10.0

Category	Sub-Category	Description
SGSN Statistics	Message Statistics - Specific Procedures	■ 3G-intra-comb-rau-fail-iu_release ■ 3G-intra-comb-rau-fail-ongoing-proc ■ 2G-intra-comb-rau-fail-ongoing-proc ■ 3G-inter-comb-rau-fail-iu_release ■ 3G-inter-comb-rau-fail-ongoing-proc ■ 2G-inter-comb-rau-fail-ongoing-proc ■ 3G-irat-comb-rej-imsi-unknown-hlr ■ 2G-irat-comb-rej-imsi-unknown-hlr ■ 3G-irat-comb-rej-illegal-ms ■ 2G-irat-comb-rej-illegal-ms ■ 3G-irat-comb-rej-illegal-me ■ 2G-irat-comb-rej-illegal-me ■ 3G-service-rej-netwk-fail ■ 3G-service-rej-imsi-unknown-at-hlr ■ 3G-service-rej-msid-not-derived-by-nwtk ■ 3G-service-rej-implicity-detach ■ 3G-service-rej-illegal-ms ■ 3G-service-rej-msg-not-compat-prot-state ■ 3G-service-rej-no-pdp-ctx-actv ■ 3G-service-rej-sem-wrong-msg ■ 3G-service-rej-unknown-cause ■ 3G-ret-paging-request ■ 2G-ret-paging-request
	Message Statistics - Common Procedures	■ 3G-ret-auth-cipher-request ■ 2G-ret-auth-cipher-request ■ 3G-ret-ptmsi-realloc ■ 2G-ret-ptmsi-realloc ■ 3G-ret-imsi-identity-request ■ 2G-ret-imsi-identity-request ■ 3G-ret-imei-identity-request ■ 2G-ret-imei-identity-request ■ 3G-ret-imeisv-identity-request ■ 2G-ret-imeisv-identity-request
	Miscellaneous Statistics	■ 3G-ptmsi-signature-mismatch-attach ■ 2G-ptmsi-signature-mismatch-attach ■ 3G-ptmsi-signature-mismatch-detach ■ 2G-ptmsi-signature-mismatch-detach ■ 3G-ptmsi-signature-mismatch-rau ■ 2G-ptmsi-signature-mismatch-rau

Table 4-16 SGSN Bulk Statistics Added in WEM Release 10.0

Category	Sub-Category	Description
SGSN Statistics	Session Management Messages	■ 3G-primary-actv-req-nrpca ■ 3G-primary-req-act-pdp ■ 3G-primary-req-act-pdp-retrans ■ 3G-primary-actv-fail ■ 2G-primary-actv-fail ■ 3G-secondary-actv-fail ■ 2G-secondary-actv-fail ■ 3G-actv-fail-phase-2-offload ■ 2G-actv-fail-phase-2-offload ■ 3G-ms-modify-rej-insufficient-resources ■ 2G-ms-modify-rej-insufficient-resources ■ 3G-ms-modify-rej-service-opt-not-supported ■ 2G-ms-modify-rej-service-opt-not-supported ■ 3G-ms-modify-rej-semantic-err-tft-operation ■ 2G-ms-modify-rej-semantic-err-tft-operation ■ 3G-ms-modify-rej-syntax-err-tft-operation ■ 2G-ms-modify-rej-syntax-err-tft-operation ■ 3G-ms-modify-rej-semnatic-err-pkt-filter ■ 2G-ms-modify-rej-semnatic-err-pkt-filter ■ 3G-ms-modify-rej-syntax-err-pkt-filter ■ 2G-ms-modify-rej-syntax-err-pkt-filter ■ 3G-ms-modify-rej-semnatic-incorrect-message ■ 2G-ms-modify-rej-semnatic-incorrect-message ■ 3G-ms-modify-rej-invalid-mand-info ■ 2G-ms-modify-rej-invalid-mand-info ■ 3G-ms-modify-rej-msg-non-existent ■ 2G-ms-modify-rej-msg-non-existent ■ 3G-ms-modify-rej-ie-non-existent ■ 2G-ms-modify-rej-ie-non-existent ■ 3G-ms-modify-rej-conditional-ie-err ■ 2G-ms-modify-rej-conditional-ie-err ■ 3G-ms-modify-rej-msg-no ■ 2G-ms-modify-rej-msg-not-compatible-prot-state ■ 3G-ms-modify-rej-rcvry-on-tmr-expiry ■ 2G-ms-modify-rej-rcvry-on-tmr-expiry ■ 3G-ms-modify-rej-prot-err-unspec ■ 2G-ms-modify-rej-prot-err-unspec ■ 3G-modify-rej-insufficient-resources ■ 3G-modify-rej-service-opt-not-supported ■ 3G-modify-rej-semantic-err-tft-operation

Table 4-16 SGSN Bulk Statistics Added in WEM Release 10.0

Category	Sub-Category	Description
SGSN Statistics	Session Management Messages	■ 3G-modify-rej-syntax-err-tft-operation ■ 3G-modify-rej-semnatic-err-pkt-filter ■ 3G-modify-rej-syntax-err-pkt-filter ■ 3G-modify-rej-semnatic-incorrect-message ■ 3G-modify-rej-invalid-mand-info ■ 3G-modify-rej-msg-non-existent ■ 3G-modify-rej-ie-non-existent ■ 3G-modify-rej-conditional-ie-err ■ 3G-modify-rej-msg-not-compatible-prot-state ■ 3G-modify-rej-rcvry-on-tmr-expiry ■ 3G-modify-rej-prot-err-unspec ■ 3G-ms-deactv-rej-rx-reg-deactv ■ 3G-ms-deactv-rej-rx-qos-not-acc ■ 3G-ms-deactv-rej-rx-nwt-fail ■ 3G-ms-deactv-rej-rx-reactivation-req ■ 3G-ms-deactv-rej-rx-no-feature-support ■ 3G-ms-deactv-rej-rx-sem-err-tft-op ■ 3G-ms-deactv-rej-rx-syn-err-tft-op ■ 3G-ms-deactv-rej-rx-unknown-ctx ■ 3G-ms-deactv-rej-rx-ctx-no-tft-already-actv ■ 3G-ms-deactv-rej-rx-mcast-grp-mem-tout ■ 3G-ms-deactv-rej-rx-sem-err-pkt-filter ■ 3G-ms-deactv-rej-rx-syn-err-pkt-filter ■ 3G-ms-deactv-rej-rx-invalid-trans-id ■ 3G-ms-deactv-rej-rx-sem-incorrect-msg ■ 3G-ms-deactv-rej-rx-inval-mand-info ■ 3G-ms-deactv-rej-rx-msg-non-existent ■ 3G-ms-deactv-rej-rx-ie-non-existent ■ 3G-ms-deactv-rej-rx-cond-ie-err ■ 3G-ms-deactv-rej-rx-prot-err-unspec ■ 3G-ms-deactv-rej-rx-apn-rest-incomap-actv-pdp ■ 3G-ms-deactv-rej-rx-msg-not-compat-prot-state ■ 3G-ms-deactv-rej-rx-rcvry-on-tmr-expiry ■ 3G-nw-deactv-rej-tx-odb ■ 3G-nw-deactv-rej-tx-mbms-cap-insuff-res ■ 3G-nw-deactv-rej-tx-llc-sndcp-fail-gb ■ 3G-nw-deactv-rej-tx-insuff-res ■ 3G-nw-deactv-rej-tx-miss-unkwn-apn ■ 3G-nw-deactv-rej-tx-unkwn-pdp-addr ■ 3G-nw-deactv-rej-tx-usr-auth-fail ■ 3G-nw-deactv-rej-tx-actv-rej-ggsn

Table 4-16 SGSN Bulk Statistics Added in WEM Release 10.0

Category	Sub-Category	Description
SGSN Statistics	Session Management Messages	■ 3G-nw-deactv-rej-tx-actv-rej-unspec ■ 3G-nw-deactv-rej-tx-service-opt-no-support ■ 3G-nw-deactv-rej-tx-service-opt-no-subs ■ 3G-nw-deactv-rej-tx-svc-opt-temp-out-order ■ 3G-nw-deactv-rej-tx-nsapi-already-used ■ 3G-nw-deactv-rej-tx-reg-deactv ■ 3G-nw-deactv-rej-tx-qos-not-acc ■ 3G-nw-deactv-rej-tx-nwt-fail ■ 3G-nw-deactv-rej-tx-reactivation-req ■ 3G-nw-deactv-rej-tx-no-feature-support ■ 3G-nw-deactv-rej-tx-sem-err-tft-op ■ 3G-nw-deactv-rej-tx-syn-err-tft-op ■ 3G-nw-deactv-rej-tx-unknown-ctx ■ 3G-nw-deactv-rej-tx-ctx-no-tft-already-actv ■ 3G-nw-deactv-rej-tx-mcast-grp-mem-tout ■ 3G-nw-deactv-rej-tx-sem-err-pkt-filter ■ 3G-nw-deactv-rej-tx-syn-err-pkt-filter ■ 3G-nw-deactv-rej-tx-invalid-trans-id ■ 3G-nw-deactv-rej-tx-sem-incorrect-msg ■ 3G-nw-deactv-rej-tx-inval-mand-info ■ 3G-nw-deactv-rej-tx-msg-non-existent ■ 3G-nw-deactv-rej-tx-ie-non-existent ■ 3G-nw-deactv-rej-tx-cond-ie-err ■ 3G-nw-deactv-rej-tx-prot-err-unspec ■ 3G-nw-deactv-rej-tx-apn-rest-incomap-actv-pdp ■ 3G-nw-deactv-rej-tx-msg-not-compat-prot-state ■ 3G-nw-deactv-rej-tx-rcvry-on-tmr-expiry ■ rab-setup-reattempt ■ rab-rel-pre-empt ■ rab-rel-utran ■ rab-rel-ue-radio-lost ■ rab-rej-unable-to-est-reloc ■ rab-rej-unknown-target-rnc ■ rab-rej-reloc-cancel ■ rab-rej-reloc-success ■ rab-rej-cypher-algo-no-support ■ rab-rej-conflict-cypher-info ■ rab-rej-failure-radio-if-proc ■ rab-rej-rel-utran-reason ■ rab-rej-utran-inactivity ■ rab-rej-time-crit-relocation

Table 4-16 SGSN Bulk Statistics Added in WEM Release 10.0

Category	Sub-Category	Description
SGSN Statistics	Session Management Messages	■ rab-rej-req-traffic-class-unavail ■ rab-rej-invalid-rab-param-val ■ rab-rej-req-max-bit-rate-unavail ■ rab-rej-req-max-bit-rate-dl-unavail ■ rab-rej-req-max-bit-rate-ul-unavail ■ rab-rej-req-gbr-unavail ■ rab-rej-req-gbr-dl-unavail ■ rab-rej-req-gbr-ul-unavail ■ rab-rej-req-trans-delay-not-achievable ■ rab-rej-inval-rab-param-combo ■ rab-rej-violation-for-sdu-param ■ rab-rej-violation-traffic-hanlde-prio ■ rab-rej-violation-for-gbr ■ rab-rej-usr-plane-ver-unsupported ■ rab-rej-iu-up-failure ■ rab-rej-reloc-alloc-expiry ■ rab-rej-reloc-failure-target-system ■ rab-rej-invalid-rdb-id ■ rab-rej-no-remaining-rab ■ rab-rej-interaction-with-other-proc ■ rab-rej-integrity-check-fail ■ rab-rej-req-type-not-supported ■ rab-rej-req-superseeded ■ rab-rej-rel-due-to-ue-sig-con-rel ■ rab-rej-res-optimization-reloc ■ rab-rej-req-info-unavail ■ rab-rej-reloc-due-to-radio-reason ■ rab-rej-reloc-unsupported-target-system ■ rab-rej-directed-retry ■ rab-rej-radio-con-with-ue-lost ■ rab-rej-rnc-unable-to-estab-all-rfcs ■ rab-rej-deciphering-keys-unavail ■ rab-rej-dedicated-assistance-data-unavail ■ rab-rej-reloc-target-not-allowed ■ rab-rej-location-reporting-congestion ■ rab-rej-reduce-load-in-serving-cell ■ rab-rej-no-radio-res-avail-in-target-cell ■ rab-rej-geran-iu-mode-failure ■ rab-rej-access-restrict-shared-nwtk ■ rab-rej-incoming-reloc-nwt-support-puesbine ■ rab-rej-traffic-target-more-source-cell

Table 4-16 SGSN Bulk Statistics Added in WEM Release 10.0

Category	Sub-Category	Description
SGSN Statistics	Session Management Messages	■ rab-rej-mbms-no-multicat-svc-for-ue ■ rab-rej-mbms-unknown-ue-id ■ rab-rej-mbms-sess-start-no-data-bearer ■ rab-rej-mbms-superseed-nnsf ■ rab-rej-mbms-ue-linking-already-done ■ rab-rej-mbms-ue-delinking-failure ■ rab-rej-tmgi-unknown ■ rab-rej-ms-unspecified-failure ■ srns-ctx-deny-rab-preempt ■ srns-ctx-deny-reloc-overall-tmr-exp ■ srns-ctx-deny-reloc-prep-tmr-exp ■ srns-ctx-deny-reloc-complete-tmr-exp ■ srns-ctx-deny-queuing-tmr-exp ■ srns-ctx-deny-reloc-triggered ■ srns-ctx-deny-unable-to-est-reloc ■ srns-ctx-deny-unknown-target-rnc ■ srns-ctx-deny-reloc-cancel ■ srns-ctx-deny-reloc-success ■ srns-ctx-deny-cypher-algo-no-support ■ srns-ctx-deny-conflict-cypher-info ■ srns-ctx-deny-failure-radio-if-proc ■ srns-ctx-deny-rel-utran-reason ■ srns-ctx-deny-utran-inactivity ■ srns-ctx-deny-time-crit-relocation ■ srns-ctx-deny-req-traffic-class-unavail ■ srns-ctx-deny-invalid-rab-param-val ■ srns-ctx-deny-req-max-bit-rate-unavail ■ srns-ctx-deny-req-max-bit-rate-dl-unavail ■ srns-ctx-deny-req-max-bit-rate-ul-unavail ■ srns-ctx-deny-req-gbr-unavail ■ srns-ctx-deny-req-gbr-dl-unavail ■ srns-ctx-deny-req-gbr-ul-unavail ■ srns-ctx-deny-req-trans-delay-not-achieve ■ srns-ctx-deny-inval-rab-param-combo ■ srns-ctx-deny-violation-for-sdu-param ■ srns-ctx-deny-violation-traffic-hanlde-prio ■ srns-ctx-deny-violation-for-gbr ■ srns-ctx-deny-usr-plane-ver-unsupported ■ srns-ctx-deny-ip-up-failure ■ srns-ctx-deny-reloc-alloc-expiry ■ srns-ctx-deny-reloc-failure-target-system

Table 4-16 SGSN Bulk Statistics Added in WEM Release 10.0

Category	Sub-Category	Description
SGSN Statistics	Session Management Messages	■ srns-ctx-deny-invalid-rdb-id ■ srns-ctx-deny-no-remaining-rab ■ srns-ctx-deny-interaction-with-other-proc ■ srns-ctx-deny-integrity-check-fail ■ srns-ctx-deny-req-type-not-supported ■ srns-ctx-deny-req-superseeded ■ srns-ctx-deny-rel-due-to-ue-sig-con-rel ■ srns-ctx-deny-res-optimization-reloc ■ srns-ctx-deny-req-info-unavail ■ srns-ctx-deny-reloc-due-to-radio-reason ■ srns-ctx-deny-reloc-unsupport-target-sys ■ srns-ctx-deny-directed-retry ■ srns-ctx-deny-radio-con-with-ue-lost ■ srns-ctx-deny-rnc-unable-to-estab-all-rfcs ■ srns-ctx-deny-deciphering-keys-unavail ■ srns-ctx-deny-dedicated-assist-data-unavail ■ srns-ctx-deny-reloc-target-not-allowed ■ srns-ctx-deny-location-reporting-congestion ■ srns-ctx-deny-reduce-load-in-serving-cell ■ srns-ctx-deny-no-radio-res-avail-target-cell ■ srns-ctx-deny-geran-iu-mode-failure ■ srns-ctx-deny-access-restrict-shared-nwtk ■ srns-ctx-deny-in-reloc-nwt-support-puesbine ■ srns-ctx-deny-traffic-target-more-src-cell ■ srns-ctx-deny-mbms-no-multicat-svc-for-ue ■ srns-ctx-deny-mbms-unknown-ue-id ■ srns-ctx-deny-mbms-sess-start-no-data-bearer ■ srns-ctx-deny-mbms-superseed-nnsf ■ srns-ctx-deny-mbms-ue-linking-already-done ■ srns-ctx-deny-mbms-ue-delinking-failure ■ srns-ctx-deny-tmgi-unknown ■ srns-ctx-deny-ms-unspecified-failure ■ srns-ctx-deny-no-response-from-rnc
SGSN Statistics	Map Statistics	■ map-mo-fwd-req-sent ■ map-mo-fwd-rsp-rcvd ■ map-mo-fwd-rsp-failed ■ map-mt-fwd-rsp-failed ■ map-ready-for-sm-req ■ map-ready-for-sm-rsp ■ map-ready-for-sm-rsp-failed ■ map-ready-for-sm-rsp-time-out

Table 4-16 SGSN Bulk Statistics Added in WEM Release 10.0

Category	Sub-Category	Description
SGSN Statistics	SMS Statistics	■ mt-sms-in-queue ■ conn-prot-data-tx ■ conn-prot-data-rx ■ conn-prot-ack-tx ■ conn-prot-ack-rx ■ conn-prot-error-tx ■ conn-prot-error-rx ■ conn-prot-error-nwt-fail-tx ■ conn-prot-error-nwt-fail-rx ■ conn-prot-error-congestion-tx ■ conn-prot-error-congestion-rx ■ conn-prot-error-invalid-tid-tx ■ conn-prot-error-invalid-tid-rx ■ conn-prot-error-invalid-semantic-tx ■ conn-prot-error-invalid-semantic-rx ■ conn-prot-error-invalid-mand-info-tx ■ conn-prot-error-invalid-mand-info-rx ■ conn-prot-error-invalid-msg-type-tx ■ conn-prot-error-invalid-msg-type-rx ■ conn-prot-error-invalid-prot-state-tx ■ conn-prot-error-invalid-prot-state-rx ■ conn-prot-error-invalid-ie-tx ■ conn-prot-error-invalid-ie-rx ■ conn-prot-error-protocol-error-tx ■ conn-prot-error-protocol-error-rx ■ conn-prot-error-undefined-cause-tx ■ conn-prot-error-undefined-cause-rx ■ conn-prot-data-dropped ■ conn-prot-ack-dropped ■ conn-prot-error-dropped ■ conn-prot-inval-tid-rcvd ■ relay-prot-data-tx ■ relay-prot-data-rx ■ relay-prot-ack-tx ■ relay-prot-ack-rx ■ relay-prot-err-tx ■ relay-prot-err-rx ■ relay-prot-smma-rx ■ relay-prot-err-unassigned-num ■ relay-prot-err-opr-determ-barring ■ relay-prot-err-call-barred

Table 4-16 SGSN Bulk Statistics Added in WEM Release 10.0

Category	Sub-Category	Description
SGSN Statistics	SMS Statistics	■ relay-prot-err-reserved ■ relay-prot-err-sm-transfer-rej ■ relay-prot-err-dest-out-of-order ■ relay-prot-err-unidentified-subs ■ relay-prot-err-facility-rej ■ relay-prot-err-unknown-subs ■ relay-prot-err-netwk-out-of-order ■ relay-prot-err-temp-fail ■ relay-prot-err-congestion ■ relay-prot-err-not-subscribed ■ relay-prot-err-not-implemented ■ relay-prot-err-interworking-err ■ relay-prot-err-res-unavail ■ relay-prot-err-mem-capacity-exceed ■ relay-prot-err-inval-ref-num-tx ■ relay-prot-err-inval-ref-num-rx ■ relay-prot-err-inval-semantic-tx ■ relay-prot-err-inval-semantic-rx ■ relay-prot-err-inval-mand-info-tx ■ relay-prot-err-inval-mand-info-rx ■ relay-prot-err-inval-msg-type-tx ■ relay-prot-err-inval-msg-type-rx ■ relay-prot-err-inval-prot-state-tx ■ relay-prot-err-inval-prot-state-rx ■ relay-prot-err-inval-ie-tx ■ relay-prot-err-inval-ie-rx ■ relay-prot-err-protocol-error-rx ■ relay-prot-err-protocol-error-tx ■ relay-prot-err-unidentified-error-tx ■ relay-prot-err-unidentified-error-rx ■ relay-prot-data-dropped ■ relay-prot-ack-dropped ■ relay-prot-error-dropped ■ relay-prot-decode-failure ■ concat-mo-sms ■ conn-prot-timer-expiry ■ tr1n-timer-expiry ■ tr2n-timer-expiry ■ conn-prot-data-retrans ■ relay-prot-msg-encode-fail ■ conn-prot-data-tx-fail

Table 4-16 SGSN Bulk Statistics Added in WEM Release 10.0

Category	Sub-Category	Description
SGSN Statistics	SMS Statistics	■ conn-prot-data-inval-tid ■ conn-prot-max-retrans-reached ■ mt-fail-conn-prot-data-no-ack-rcvd ■ mt-fail-no-db-rec ■ mt-fail-fwd-busy-subs ■ mt-fail-fwd-detached-subs ■ mt-fail-mt-queue-full

Web Element Manager Path:

Accounting\View/Graph Bulk Statistics\Dialog Boxes\Counter Categories & Analysis Counters List

CSCF Bulk Statistics

The following CSCF Bulk Statistics were added for release 10.0.

Table 4-17 IMS CSCF Bulk Statistics Added in WEM Release 10.0

Statistic Category	Description
CSCF Statistics	■ perf-att-3rdparty-reg ■ perf-succ-3rdparty-reg ■ perf-fail-3rdparty-reg ■ perf-fail-3rdparty-reg-401 ■ perf-fail-3rdparty-reg-403 ■ perf-fail-3rdparty-reg-404 ■ perf-fail-3rdparty-reg-420 ■ perf-fail-3rdparty-reg-500 ■ perf-fail-3rdparty-reg-other ■ de2a-session-init ■ de2a-session-active ■ de2a-udr-sent ■ de2a-uda-received ■ de2a-uda-err-3xxx ■ de2a-uda-parse-err ■ de2a-udr-err ■ dereg-resp-4xxrx ■ dereg-resp-4xxtx ■ dereg-resp-5xxrx ■ dereg-resp-5xxtx ■ dereg-resp-6xxrx ■ dereg-resp-6xxtx ■ reg-resp-4xxrx ■ reg-resp-4xxtx ■ reg-resp-5xxrx ■ reg-resp-5xxtx ■ reg-resp-6xxrx ■ reg-resp-6xxtx ■ rereg-resp-4xxrx ■ rereg-resp-4xxtx ■ rereg-resp-5xxrx ■ rereg-resp-5xxtx ■ rereg-resp-6xxrx ■ rereg-resp-6xxtx ■ dpeca-tot-uncorr-aaa ■ dpeca-tot-uncorr-sta

Web Element Manager Path

Accounting\View/Graph Bulk Statistics\Dialog Boxes\Counter Categories & Analysis Counters List

Context Bulk Statistics

The following context bulk statistics were added for release 10.0.

Table 4-18 Context Bulk Statistics Added in WEM Release 10.0

Statistic Category	Description
DNS Client	■ dns-primary-ns-a-atmpts ■ dns-primary-ns-a-fails ■ dns-primary-ns-a-succs ■ dns-primary-ns-aaaa-atmpts ■ dns-primary-ns-aaaa-fails ■ dns-primary-ns-aaaa-succs ■ dns-primary-ns-naptr-atmpts ■ dns-primary-ns-naptr-fails ■ dns-primary-ns-naptr-succs ■ dns-primary-ns-srv-atmpts ■ dns-primary-ns-srv-fails ■ dns-primary-ns-srv-succs ■ dns-secondary-ns-a-atmpts ■ dns-secondary-ns-a-fails ■ dns-secondary-ns-a-succs ■ dns-secondary-ns-aaaa-atmpts ■ dns-secondary-ns-aaaa-fails ■ dns-secondary-ns-aaaa-succs ■ dns-secondary-ns-naptr-atmpts ■ dns-secondary-ns-naptr-fails ■ dns-secondary-ns-naptr-succs ■ dns-secondary-ns-srv-atmpts ■ dns-secondary-ns-srv-fails ■ dns-secondary-ns-srv-succs

Card Bulk Statistics

The following Card bulk statistics were added for release 10.0.

Table 4-19 Card Bulk Statistics Added in WEM Release 10.0

Statistic Category	Description
Card	■ npuutil-now ■ npuutil-5minave ■ npuutil-15minave ■ npuutil-rxpkts-5secave ■ npuutil-rxbytes-5secave ■ npuutil-txpkts-5secave ■ npuutil-txbytes-5secave ■ npuutil-rxpkts-5minave ■ npuutil-rxbytes-5minave ■ npuutil-txpkts-5minave ■ npuutil-txbytes-5minave ■ npuutil-rxpkts-15minave ■ npuutil-rxbytes-15minave ■ npuutil-txpkts-15minave ■ npuutil-txbytes-15minave

Support for Sharing Generated Bulk Statistics Reports

WEM now supports the sharing of bulk statistics reports generated from the Bulk Statistics Report Configuration Dialog Box. A **Shared Query** check box has been added to this dialog box. If the **Shared Query** box is left unchecked, only the user who generated the report will be able to view the results. If the **Shared Query** box is checked, the generated report will be available to all users.

Web Element Manager Path:

Accounting\Bulk Statistics\Bulks Statistics Report Configuration

CHAPTER 5
PERFORMANCE MANAGEMENT

This section contains additions and changes made to the performance commands available in this release. Topics covered in this chapter are:

New Commands

This section contains performance management commands that are new in Release 10.0. New commands in this version are divided into the following sections:

Common Commands - New in Release 10.0

The following common commands are new in Release 10.0.

threshold diameter diameter-retry-rate

This command configures Diameter Retry Rate threshold for generating alerts or alarms based on the percentage of Diameter requests that were retried during the polling interval.

CLI (Global Configuration Mode)

`threshold diameter diameter-retry-rate` *`high_thresh`* **`[ clear`** *`low_thresh`* **`]`**

`default threshold diameter diameter-retry-rate`

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

threshold monitoring diameter

This command enables/disables threshold monitoring for Diameter thresholds.

CLI (Global Configuration Mode)

`[ default | no ] threshold monitoring diameter`

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

threshold poll diameter-retry-rate

This command configures the polling interval for Diameter Retry Rate threshold.

CLI (Global Configuration Mode)

`threshold poll diameter-retry-rate interval` *`duration`*

`default threshold poll diameter-retry-rate interval`

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

Content Filtering Commands - New in Release 10.0

The following Content Filtering commands are new in Release 10.0.

None for this release.

ASN Gateway Commands - New in Release 10.0

The following ASGW command has been enhanced in Release 10.0.

show rohc statistics

The following options have been added to this command in 10.0:

- **sessmgr instance <value>** displays ROHC statistics for a specified session manager instance. Must be followed by a session manager instance number.
- **asngw-service** displays ASNGW service-related statistics for a specific ASNGW service. Must be followed by the ASNGW service name.

CLI Exec Mode

show rohc statistics [sessmgr instance <value> | pdsn-service | asngw-service] < name >]

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

ECS Commands - New in Release 10.0

The following ECS commands are new in Release 10.0.

None for this release.

Firewall Commands - New in Release 10.0

The following Stateful Firewall commands are new in Release 10.0.

None for this release.

GGSN Commands - New in Release 10.0

The following GGSN commands are new in Release 10.0.

show gtpu statistics

A new command displaying GTP-U statistics/counters was added in this release.

CLI (Exec Mode)

show gtpu statistics [gtpumgr-instance *number* **] [gtpu-service** *name* **| peer-address** *ip_address* **]**

HA Commands - New in Release 10.0

The following HA commands are new in Release 10.0.

None for this release.

NAT Commands - New in Release 10.0

The following NAT commands are new in Release 10.0.

None for this release.

PDIF Commands - New in Release 10.0

The following PDIF commands are new in Release 10.0.

None for this release.

PDN Gateway Commands - New in Release 10.0

The following P-GW commands are new in Release 10.0.

show gtpu statistics

A new command displaying GTP-U statistics/counters was added in this release.

CLI (Exec Mode)

show gtpu statistics [gtpumgr-instance *number* **] [gtpu-service** *name* **| peer-address** *ip_address* **]**

PDSN Commands - New in Release 10.0

The following PDSN commands are new in Release 10.0.

None for this release.

Peer-to-Peer - New in Release 10.0

The following P2P commands are new in Release 10.0.

Serving Gateway Commands - New in Release 10.0

The following S-GW commands are new in Release 10.0.

show gtpu statistics

A new command displaying GTP-U statistics/counters was added in this release.

CLI (Exec Mode)

show gtpu statistics [gtpumgr-instance *number* **] [gtpu-service** *name* **| peer-address** *ip_address* **]**

Modified Commands

This section contains performance management commands that have been modified in Release 10.0. Modified commands in this version are divided into the following sections:

Common Commands - Modified in Release 10.0

The following common commands have been modified in Release 10.0.

clear active-charging analyzer statistics

This command clears protocol analyzer statistics. The following protocol options were added to this command:

- **pptp**
- **tftp**

CLI (Exec Mode)

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

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

show active-charging analyzer statistics

This command displays protocol analyzer statistics. The following protocol options were added to this command:

- **pptp**
- **tftp**

CLI (Exec Mode)

show active-charging analyzer statistics [name *protocol* **[verbose]] [| { grep** *grep_options* **| more }]**

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

show active-charging credit-control statistics group default

This command displays statistics for Diameter/RADIUS Prepaid Credit Control Service in the ACS service. The output of this command includes the following new fields:

- Permanent Failures
- Transient Failures

CLI (Exec Mode)

show active-charging credit-control statistics group default

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

show active-charging edr-udr-file statistics

This command displays CDR flow control and EDR and UDR file related information. The output of this command includes the new field “Num of times PUSH Failed”, which indicates the number of times an EDR/UDR push attempt failed, once each in the Overall Statistics, Primary Server Statistics, and Secondary Server Statistics categories.

CLI (Exec Mode)

show active-charging edr-udr-file { flow-control-counters [verbose] | statistics } [| { grep *grep_options* **| more }]**

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

show active-charging flows type

This command displays information on active charging flows. The following protocol type options were added to this command:

- **pptp**
- **tftp**

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** *protocol_type* **] } [| { grep** *grep_options* **| more }]**

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

show active-charging service all

This command has been enhanced to display the “diameter mscc-final-unit-action terminate” configuration.

CLI (Exec Mode)

show active-charging service { all | name *acs_service_name* **} [| { grep** *grep_options* **| more }]**

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

show active-charging sessions

This command displays Active Charging session statistics. The following protocol type options were added to this command:

- **pptp**
- **tftp**

The output of the command displays statistics for the pptp/tftp protocol:

CLI (Exec Mode)

show active-charging sessions [full [wide] | summary | display-dynamic-charging-rules | dynamic-charging] { [all] | [*filter_keyword* **] + } [| { grep** *grep_options* **| more }]**

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

show ims-authorization sessions full all

This command displays information, configuration, and statistics of sessions active in IP Multimedia Subsystem (IMS) authorization service.

The output of this command includes the following new field:

- Bearer Control Mode

CLI (Exec Mode)

show ims-authorization sessions full all

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

Content Filtering Commands - Modified in Release 10.0

The following Content Filtering commands have been modified in Release 10.0.

ECS Commands - Modified in Release 10.0

The following ECS commands have been modified in Release 10.0.

Firewall Commands - Modified in Release 10.0

The following Stateful Firewall commands have been modified in Release 10.0.

show active-charging firewall statistics verbose

This command displays the Active Charging Stateful Firewall statistics. The output of this command now includes the following new fields to display the SIP ALG statistics:

- ALG statistics:
  - Packets dropped by SIP ALG
  - Packets injected by SIP ALG

CLI (Exec Mode)

show active-charging firewall statistics [callid *call_id* **| domain-name** *domain_name* **| nat-realm** *nat_realm* **| protocol { icmp | ip | other | tcp | udp } | username** *user_name* **] [acsmgr instance** *instance_id* **] [verbose] [| { grep** *grep_options* **| more }]**

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

show active-charging fw-and-nat policy name

This command displays the Firewall and NAT policy information. The output of this command now includes the following new fields to display the threshold on the number of TCP Reset messages sent by the subscriber:

- TCP RST Message Threshold
- TCP RST Message Threshold Value

CLI (Exec Mode)

show active-charging fw-and-nat policy { { { all | name *fw-nat-policy* **}[service name** *acs_service* **] } | { statistics { all | name** *fw-nat-policy* **} } } [| { grep** *grep_options* **| more }]**

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

GGSN Commands - Modified in Release 10.0

The following GGSN commands have been modified in Release 10.0.

show gtpp group statistics

New counter `Force File rotation by time-interval` added to the output of this command to display the status of force rotation of CDR files:

CLI (Exec Mode)

show gtpp group [name *gtpp_group_name* **| all]] [| { grep** *grep_options* **| more }]**

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

show gtpp storage-server local file statistics

New counter `Forced (0 CDRs)` added to the output of this command under `File Rotation Type` group to track of the number of zero-CDR files created at the local storage:

CLI (Exec Mode)

show gtpp storage-server [counters { all | group name *name***} | group name** *name***| local file { counters { all | group name** *name***} | statistics [group name** *name***] } | status [verbose] | streaming { counters { all | group name** *name***} | statistics [group name** *name***] }] [| { grep grep_options | more }]**

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

show gtpp statistics

New counter `CDRs purged by dead-server suppress-cdrs` added to the output of this command to track the purged DRTs on all GTPP group when **gtpp dead-server suppress-cdrs** command is configured:

CLI (Exec Mode)

show gtpp statistics [cgf-address *cgf_address* **] [| { grep** *grep_options* **| more }]**

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

HA Commands - Modified in Release 10.0

The following HA commands have been modified in Release 10.0.

None for this release.

NAT Commands - Modified in Release 10.0

The following NAT commands have been modified in Release 10.0.

show active-charging nat statistics

This command displays NAT realm statistics.

The optional keyword **summary** was added to this command.

When the *nat_realm* specified is a “pool group” and the **summary** option is used, summary statistics for each pool in the specified “pool group” is displayed.

When the *nat_realm* specified is a pool and the **summary** option is NOT used, all available statistics for the specified pool is displayed.

When the *nat_realm* specified is a “pool group” and the **summary** option is NOT used, all available statistics of each pool in the specified “pool group” is displayed.

The following fields were added to the output of this command:

- NAT Realm Utilization
  - Port-Chunk size
- Statistics
  - Average TCP port usage
  - Average UDP port usage
  - Average Others port usage

CLI (Exec mode)

show active-charging nat statistics [nat-realm *nat_realm* **[summary]] [| { grep** *grep_options* **| more }]**

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

show active-charging nat statistics

This command displays NAT realm statistics.

The following fields were added to the output of this command:

- Port-Chunks distribution
  - Max no.of chunks used
  - Total no.of subscribers
  - Current no.of subscribers

CLI (Exec mode)

show active-charging nat statistics [nat-realm *nat_realm* **[summary]] [| { grep** *grep_options* **| more }]**

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

show active-charging service

This command displays the Active Charging Service details.

The output of this command includes the following new field, which indicates the configured ALG media idle timeout value:

- ALG Media Idle Timeout

CLI (Exec mode)

show active-charging service all { all | name *acs_service* **} [| { grep** *grep_options* **| more }]**

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

show active-charging firewall statistics verbose

This command displays the Active Charging Stateful Firewall statistics. The output of this command now includes the following new fields to display the SIP ALG statistics:

- ALG statistics:
  - Packets dropped by SIP ALG
  - Packets injected by SIP ALG

CLI (Exec Mode)

show active-charging firewall statistics [callid *call_id* **| domain-name** *domain_name* **| nat-realm** *nat_realm* **| protocol { icmp | ip | other | tcp | udp } | username** *user_name* **] [acsmgr instance** *instance_id* **] [verbose] [| { grep** *grep_options* **| more }]**

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

show active-charging sessions summary

This command displays the Active Charging Service details.

The following field was added to the output of this command to show the Active Charging sessions which are having active TFTP sessions:

- Current TFTP Sessions

CLI (Exec mode)

show active-charging sessions [full [wide] | summary | display-dynamic-charging-rules | dynamic-charging] { [all] | [*filter_keyword* **] + } [| { grep** *grep_options* **| more }]**

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

show active-charging analyzer statistics name tftp

This command displays Active Charging protocol analyzer statistics for the TFTP analyzer. The following new fields are added to the output of this command to display different statistics that are captured by the TFTP Analyzer:

- ACS TFTP Session Stats:
  - Total Uplink Bytes
  - Total Downlink Bytes
  - Total Uplink Packets
  - Total Downlink Packets
  - Total Read Sessions
  - Total Write Sessions
  - Total Invalid Control Packets
  - Total Invalid Data Packets
  - Total Packets with Unknown Request Type

CLI (Exec Mode)

show active-charging analyzer statistics name tftp [verbose] [| { grep *grep_options* **| more }]**

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

show active-charging subsystem all

This command displays service and configuration counters for the active charging service. The following new fields are added to the output of this command:

- Total TFTP flows
- Current TFTP flows

CLI (Exec Mode)

show active-charging subsystem { all | facility acsmgr { all | instance *instance_value* **} } [rulebase** *rulebase_name* **] | [| { grep** *grep_options* **| more }]**

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

show active-charging sessions full

This command displays statistics for specific active charging service sessions. The following new field is added to the output of this command:

- Current TFTP flows

CLI (Exec Mode)

show active-charging sessions [full [wide] | summary | display-dynamic-charging-rules | dynamic-charging] {[all] | [*filters_keyword* **] + } [| { grep** *grep_options* **| more }]**

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

show subscribers full

This command displays all available subscriber information. The following new field is added to the output of this command to support discontiguous address ranges on NAT pool:

- (<pool_name>)

CLI (Exec Mode)

show subscribers full [*command_keyword* **] [** *filter_keywords* **] [| { grep** *grep_options* **| more }]**

Web Element Manager Path

This functionality is not supported at this time on the Web Element Manager.

PDIF Commands - Modified in Release 10.0

The following PDIF commands have been modified in Release 10.0.

None for this release.

PDN Gateway Commands - Modified in Release 10.0

The following P-GW commands have been modified in Release 10.0:

show pgw-service statistics

The following counters were added to the output of this command:

- Total bearers active
  - Default bearers
- Total bearers setup
  - Dedicated bearers
- Network initiated release
  - Admin disconnect
  - GTP-U error ind
  - SGW Path failure
  - MME Initiated release
- Dedicated bearers
  - UE-req reject
  - Network-req reject
- Total bearers modification failure
  - UE-initiated mod failed
  - Network-initiated mod failed
    - Semantic err in TFT oper
    - Syntact err in TFT oper
    - Semantic err in pkt filter
    - Syntact err in pkt filter
- Subscriber Data Statistics
  - Uplink/Downlink/Packet/Bytes/Forwarded/Dropped
    - Standard QCI (Non-GBR)
    - Standard QCI (GBR)
    - Non-GBR
    - GBR

CLI (Exec Mode

show pgw-service { all | name *service_name* **| statistics { all | name** *service_name* **} }**

PDSN Commands - Modified in Release 10.0

The following PDSN commands have been modified in Release 10.0.

None for this release.

Peer-to-Peer Commands - Modified in Release 10.0

The following Peer-to-Peer commands have been modified in Release 10.0.

None for this release.

Session Control Manager Commands - Modified in Release 10.0

The following SCM commands have been modified in Release 10.0.

None for this release.

Serving Gateway Commands - Modified in Release 10.0

The following S-GW commands have been modified in Release 10.0:

show sgw-service statistics

The following counters were added to the output of this command:

- PDNs Rejected Reason:
  - Path Failure S11
  - Path Failure S1-U
  - Path Failure S5
  - Path Failure S5-U
- PDNs Rejected Reason:
  - Newcall Policy
  - Congestion
  - License
  - Overload

CLI (Exec Mode)

show sgw-service statistics { all | name *service_name* **}**

Obsoleted Commands

This section contains performance management commands that have been obsoleted in Release 10.0. Obsoleted commands in this version are divided into the following sections:

Common Commands - Obsoleted from Release 10.0

The following common commands have been obsoleted in Release 10.0.

Content Filtering Commands - Obsoleted from Release 10.0

The following Content Filtering commands have been obsoleted in Release 10.0.

None for this release.

ECS Commands - Obsoleted from Release 10.0

The following ECS commands have been obsoleted in Release 10.0.

None for this release.

Firewall Commands - Obsoleted from Release 10.0

The following Stateful Firewall commands have been obsoleted in Release 10.0.

None for this release.

GGSN Commands - Obsoleted from Release 10.0

The following GGSN commands have been obsoleted in Release 10.0.

None for this release.

HA Commands - Obsoleted from Release 10.0

The following HA commands have been obsoleted in Release 10.0.

None for this release.

NAT Commands - Obsoleted from Release 10.0

The following NAT commands have been obsoleted in Release 10.0.

None for this release.

PDSN Commands - Obsoleted from Release 10.0

The following PDSN commands have been obsoleted in Release 10.0.

None for this release.

Peer-to-Peer Commands - Obsoleted from Release 10.0

The following Peer-to-Peer commands have been obsoleted in Release 10.0.

None for this release.

GTPP Storage Server Changes

The following commands have been modified in Release 10.0.

Web Element Manager Changes

This section describes the Performance Management features added in Release 10.0.

DNS Client Information Support for IMS

WEM now provides performance information for IMS DNS clients. Information can be obtained by System and context, query type, query name, and client name. Information provided includes:

- DNS Client Statistics:
  - Usage Statistics
  - Cache Statistics
  - Resolver Statistics
- Cache Information:
  - Query Type
  - Query Name
  - TTL
  - Answer
- Query Information:
  - Query Type
  - Query Name
  - TTL
  - Answer

Web Element Manager Path

Performance\IMS\DNS Client Information

CHAPTER 6
SECURITY MANAGEMENT

This section contains additions and changes made to the security features available in Release 10.0.

Security Enhancements

New Commands

The following new commands were added for Release 10.0.

None for this release.

Modified Commands

The following commands were modified in Release 10.0.

None for this release.

Obsoleted Commands

The following commands were obsoleted in Release 10.0.

None for this release.

Web Element Manager Security Enhancements

This section describes the Web Element Manager security enhancements provided in release 10.0.

Support for Aggregate Audit Attributes

WEM now supports aggregating multiple audit attributes into a single attribute through the use of mathematical operators.

WEM uses the values derived from selected Command Line Interface (CLI) command output and generates an aggregate value based on the mathematical operators used with the CLI commands. For example, if you wanted to generate a report that calculates the peak license usage as a percentage of the available licenses you would define three attributes to provide the percentage value.

- Attribute 1 = peak license usage (derived from a CLI command output)
- Attribute 2 = available licenses (derived from a CLI command output)
- Attribute 3 = license usage = (Attribute1/Attribute2) x 100

Attributes 1 and 2 are combined to define an aggregate attribute (Attribute 3) via the use of mathematical operators.

Web Element Manager Path

Security\Configuration Audit\Query Information\Configuration Audit Query Information Dialog Box\Add\Add Configuration Audit Query Dialog Box\Add Aggregate

Support for Field Separators When Defining Audit Attributes

WEM now supports the parsing of audit attributes using a using a user-defined field separator and secondary field separators for use with the Configuration Audit feature.

For example, if the audit attribute output is “radius port 1812 server 127.0.0.1” and only port and server is required, then the field separator could be entered as “ ” (space) and “3,5” could be specified as fields. In addition, if you want further filtering, the parameters can be separated by a special character, for example, “|”. The final output in this example would be “1812|127.0.0.1”.

Web Element Manager Path

Security\Configuration Audit\Query Information\Configuration Audit Query Information Dialog Box\Add\Add Configuration Audit Query Dialog Box

Support for Additional Email Configuration of Audit Report Distribution

WEM now supports the editing of the audit report’s email title and body. When adding or modifying a mailing configuration, the user can enter a subject line for the email, as well as introductory text in the body of the email itself. In addition, WEM provides an option to include a list of attributes in the email body, which will be displayed in alphabetical order if the attributes differ from the previous audit for the same system.

Web Element Manager Path

- Security\Configuration Audit\Schedule\Configuration Audit Schedule Dialog Box\Configure Mailing\Add

and

- Security\Configuration Audit\Schedule\Configuration Audit Schedule Dialog Box\Configure Mailing\Modify

Validation of Configuration Audit Attributes

WEM now supports the validation of audit attribute results against a user-defined value. This feature is useful if system administrators would like to monitor whether the outpout of the attribute is in compliance with the recommended value for the attribute.

For example, if the attribute *RADIUS Max Retry* is defined by the user as **0**, the audit result will indicate shich systems are in compliance with that setting.

If any user-defined value is not in compliance, it will be highlighted in the XLS audit report next to the user-defined value.

Web Element Manager Path

Security\Configuration\Query Information\Configuration Audit Query Information Dialog Box\Add