Cisco ASR 5000 Series Release 10.0 to Release 11.0 Change Reference

Version 11.0

Generally Available 01-14-2011

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-23919-02

Cisco ASR 5000 Series Release 10.0 to Release 11.0 Change Reference

TABLE OF CONTENTS

Chapter 2: Fault Management

Chapter 3: Configuration Management

Chapter 4: Accounting Management

Chapter 5: Performance Management

Chapter 6: Security Management

ABOUT THIS GUIDE

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

Conventions Used

The following tables describe the conventions used throughout this documentation.

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

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

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

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

Contacting Customer Support

Use the information in this section to contact customer support.

For New Customers: Refer to the support area of http://www.cisco.com for up-to-date product documentation or to submit a service request. A valid username and password is required to this site. Please contact your local sales or service representative for additional information.

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

IMPORTANT

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

CHAPTER 1
NEW FEATURE SUMMARY

This guide identifies features and functionality added to or modified for 11.0 software releases. Topics covered in this chapter are:

Related Documents

Additional information on these items is located in the documents provided with the 11.0 release, see the table below.

Table 1-1 11.0 Release Documentation

Document	Part Number
Cisco ASR 5000 Series Product Overview Guide	OL-24215-01
Cisco ASR 5000 Series SNMP MIB Reference	OL-23912-02
Cisco ASR 5000 Series Gateway GPRS Support Node Administration Guide	OL-23913-02
Cisco Web Element Manager Installation and Administration Guide	OL-24216-01
Cisco ASR 5000 Series Command Line Interface Reference	OL-23916-02
Cisco ASR 5000 Series Enhanced Charging Services Administration Guide	OL-23917-02
Cisco ASR 5000 Series Session Control Manager Administration Guide	OL-24217-01
Cisco ASR 5000 Series AAA and GTP Interface Administration and Reference	OL-23918-02
Cisco ASR 5000 Series Release 10.0 to Release 11.0 Change Reference	OL-23919-02
Cisco ASR 5000 Series Content Filtering Services Administration Guide	OL-23920-02
Cisco ASR 5000 Series Peer-to-Peer Detection Administration Guide	OL-23921-02
Cisco ASR 5000 Series Personal Stateful Firewall Administration Guide	OL-24220-01
Cisco ASR 5000 Series Thresholding Configuration Guide	OL-24221-01
Cisco ASR 5000 Series Serving GPRS Support Node Administration Guide	OL-23922-02
Cisco ASR 5000 Series System Administration Guide	OL-23923-02
Cisco ASR 5000 Series Enhanced Feature Configuration Guide	OL-23924-02
Cisco ASR 5000 Series Packet Data Network Gateway Administration Guide	OL-23925-01
Cisco ASR 5000 Series Serving Gateway Administration Guide	OL-23962-01
Cisco ASR 5000 Series Mobility Management Entity Administration Guide	OL-24222-01
Cisco ASR 5000 Series Statistics and Counters Reference	OL-23927-02
Cisco ASR 5000 Series Network Address Translation Administration Guide	OL-24223-01
Cisco ASR 5000 Series Mobility Unified Reporting System Installation and Administration Guide	OL-24224-01
Cisco ASR 5000 Series 3G Home NodeB Gateway Administration Guide	OL-24225-01
Cisco ASR 5000 Series Packet Data Gateway/Tunnel Termination Gateway Administration Guide	OL-24226-01

Common Features in Release 11.0

This section provides information on new features that are common to products in Release 11.0.

ASR 5000 CLI access

The CLI command “cli access” has been updated with a new option “show-configuration” to configure the access level for the SHOW command “show configuration”. This option has been specially included to empower the operator-level users to be capable of entering context level/config mode and execute the SHOW Config Mode related commands.

The default access level for the SHOW command “show configuration” will be “operator”. Earlier the operators were given read-only privileges to a larger subset of the Exec Mode commands

Call Termination on Event Triggers - Behavioral Change

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

In the earlier releases, when NO_EVENT_TRIGGERS was sent along with other event triggers present in CCA/RAR message, the call was terminated automatically.

In the current release, the call continues without any termination even when the NO_EVENT_TRIGGERS is sent along with other event triggers for the Event-Trigger AVP.

Exclusion of Bearer AVP in RAA Message - Behavioral Change

This Diameter-related behavioral change is applicable to GGSN.

In the earlier releases, the Bearer-Identifier AVP was part of the Re-Auth-Answer (RAA) message in dpca-custom9 dictionary.

In the current release, per the standard spec, the Bearer-Identifier AVP is removed from the RAA message.

Gx - Bearer Binding - Behavioral Change

This behavioral change is applicable to GTP-PGW.

In earlier releases, ECS used only the Priority-Level part of ARP byte for bearer binding, (along with QCI).

Now the entire ARP byte for bearer binding (along with QCI) is used. Since the capability and vulnerability bits are optional in a dynamic rule, if a dynamic rule is received without these flags, it is assumed that the capability bit is set to 1 (disabled), and vulnerability bit is set to 0 (enabled). For predefined rules, currently configuring these two flags is not supported, so now all predefined rules are assumed to have capability bit set to 1 (disabled) and vulnerability bit set to 0 (enabled).

Gx-Gy Interaction - Behavioral Change

This change pertains to deferring quota request on Gy for Dynamic URLs with online enabled AVP received over Gx, and applies to all products in Gy.

In the earlier releases, when dynamic rule with Online AVP enabled is received on Gx interface, GGSN automatically requests quota with corresponding RG on Gy to OCS without traffic matching the dynamic rule. Should there be many rules provisioned in CCR-I, this will lead to massive funds reservation in the OCS system and potentially blocking the subscriber from access to other services.

In this release, CLI support is added to enable deferring asking for quota unless there is some traffic matching the dynamic-rule with ONLINE enabled received on Gx. The default setting is to request quota immediately in the CCR sent to Gy on receiving a dynamic rule with ONLINE enabled (on-receiving-rule).

Gx - Installation of Dynamic Rules - Behavioral Change

In this release, IMSA and ECS allow the PCRF to install two (or more) dynamic rules with the same precedence value. In earlier releases, if distinct dynamic rules have the same precedence value, rules with duplicate priorities were detected and rejected. In this release that check has been removed. Note that only one rule will be matched, but all will be attempted for a match until a match is found. If a rule gets modified, or rebound, that leads to it being removed from the list of rules to match, and if the modification/rebinding succeeds, being reinserted in the list. So that would probably make it the last rule at that priority, till a new rule gets inserted at that priority.

This change applies for all Gx scenarios irrespective of product type.

Gx - PCEF-based Rule Binding - Behavioral Change

This behavioral change is applicable to GGSN/GTP-PGW with PCEF-based rule binding.

For PCEF bound dynamic/predefined rules, ECS now checks for MBR/GBR of a dynamic/predefined rule before using it for PCEF binding. All rules (dynamic as well as predefined) have to have an MBR associated with them and all rules with GBR QCI should also have GBR configured. This is irrespective of Rel. 7 or Rel. 8 Gx, and irrespective of GGSN/G-PGW. So for predefined rules, appropriate peak-data-rate and committed-data-rate must be configured as per the QCI being GBR QCI or non-GBR QCI.

Gx - PCEF Binding - Change of Rulebase via Gx - Behavioral Change

This behavioral change is applicable to GGSN/GTP-PGW (PCEF binding scenarios).

In this release, ECS allows change of rulebase via Gx for PCEF binding scenarios. When the old rulebase goes away, all the rules that were installed from that rulebase are removed. This may lead to termination of a few bearers (PDP contexts) if they are left without any rules. If there is a Gx message that changes the rulebase, and also activates some predefined rules, the rulebase change is made first, and the rules are activated from the new rulebase. Also, the rulebase now applies to the entire call. All PDP contexts (bearers) in one call use the same rulebase.

Gx - Rule-Activation-Time, Rule-Deactivation-Time, and Revalidation-Time AVPs - Behavioral Change

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

In earlier releases, Rule-Activation-Time/ Rule-Deactivation-Time/ Revalidation-Time AVP is successfully parsed only if its value corresponds to a later time than the current IPSG time, else the AVP and entire message is rejected.

In this release Rule-Activation-Time/ Rule-Deactivation-Time/ Revalidation-Time AVP is successfully parsed only if its value corresponds to current time or a later time than the current IPSG time, else the AVP and entire message is rejected.

Gx - Volume Reporting over Gx - Immediate Usage Reporting Support - Behavioral Change

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

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

In this release this behavior is modified as per 3GPP R9 29.212. PCEF resets the usage after immediate reporting and sends the accumulated usage since the last report.

Handling of PCRF Charging Rule - Behavioral Change

This Diameter-related behavioral change is applicable to all products that use the R8Gx / Gxx / Ty / R7Gx interface.

In the earlier releases, the length of the charging rule name constructed by PCRF was limited to 32 bytes. When the length of charging rule name was between 32 and 64 bytes, then a charging rule report with RESOURCES_LIMITATION as Rule-Failure-Code was sent.

In the current release, the maximum valid length for the charging rule name is 63 bytes. The charging rule report with RESOURCES_LIMITATION as Rule-Failure-Code will be sent only when the length of the rule name is between 63 and 128 bytes. When the charging rule name length exceeds 128 bytes no charging rule report will be sent.

QoS-Class-Identifier AVP Values - Behavioral Change

This Diameter-related behavioral change is applicable to all products using R8 Gx or R8 Gxx.

In the earlier releases, the QoS-Class-Identifier AVP is of type ENUM and was displayed as QCI_1 to QCI_9 for R8 Gx/Gxx interface.

In the current release, the type values “128-254: Operator specific” are also considered as valid values for the QoS-Class-Identifier AVP in order to comply with the standard requirements.

Trigger-Type AVP

This Diameter-related change is applicable to GTP and PMIP PGW Gy.

In this release the Trigger-Type AVP supports the new value CHANGE_IN_SERVING_NODE(61). This value is used to indicate that a change in serving node shall cause the Credit Control client to ask for a re-authorization of the associated quota.

Triggering of SGSN_Change During P-GW Handover

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

In earlier releases, in case of P-GW with GnGp access, after a P-GW mode to GGSN mode handover, SGSN_CHANGE(0), Event-Trigger, and 3GPP-SGSN-Address were sent.

In this release, since SGSN-Address is invalid in the case of P-GW with S5/S8, SGSN_CHANGE(0) would not be meaningful after a P-GW mode to GGSN mode handover. Therefore, AN_GW_CHANGE (21), Event-Trigger, and IPv4 SGSN address will be sent in the AN-GW-Address AVP.

ASN GW Features in Release 11.0

None for this release.

Content Filtering in Release 11.0

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

ON / OFF License Support for CF

The current release supports the following new license for CF. This new license is independent of the old session counting license.

[600-20-0109] Integrated Content Filtering Provisioned Service, 1k Sessions

This is implemented as an on / off license.

TCP Proxy Functionality

The CF solution utilizes the services of TCP Proxy to receive all the packets of a response and then takes appropriate actions after rating the response. This functionality can be implemented for HTTP1.0, HTTP1.1 and WAP2.0 protocols.

IMPORTANT

For the dynamic CF to be functional, the TCP Proxy feature is required.

When TCP Proxy is configured to work with dynamic CF, the CF solution starts to buffer the packets in a temporary memory until the complete HTTP response page is received. When the entire response cannot be buffered, apply the action specified in default policy. If no default policy is specified, then allow the content to pass through. The complete response will be reassembled at CF and sent for dynamic rating only if the HTTP response code is in the 2xx range. Otherwise, the CF will stream the response back to MS with no further CF action.

TCP Proxy must be enabled at the rulebase level. When enabled in a rulebase, it is applied for subscribers using that rulebase. For information on how to configure TCP Proxy, refer to the Configuring TCP Proxy for CF section in the Content Filtering Service Configuration chapter.

IMPORTANT

Dynamic CF is performed only on those responses which are either rated DYNAM or UNKNOW during static rating.

For more information on this feature implementation in relation to CF, refer to the *Content Filtering Services Administration Guide*.

ECS Features in Release 11.0

This section provides information on new features in the Enhanced Charging Service in Release 11.0.

None for this release.

ESS Features in Release 11.0

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 11.0

This section provides information for new features in the Stateful Firewall product in Release 11.0.

ICMP Traceroute

Firewall now supports ICMP Traceroute to handle ICMP packets with type value 30 that were being dropped. ICMP packets with ICMP type value 30 are called ICMP Traceroute packets.

For more information, please refer to the *Personal Stateful Firewall Administration Guide.*

ICMP Echo ID

In this release, it is possible to allow/deny the ICMP echo packets having identifier value zero. By default, these packets are allowed. This feature will be effective only if Firewall is enabled (Firewall or Firewall+NAT) for a call. For only NAT enabled calls, there is no change in the behavior. Configuration is available only if Firewall license is present.

For more information, please refer to the *Personal Stateful Firewall Administration Guide.*

TCP Partial Connection Timeout

In this release, idle timeout for TCP transitory connections can be configured. This timeout is applied for TCP transitory connections (partially open) in case of Firewall enabled calls. The “transitory connection idle-timeout” for a NAT is defined as the minimum time a TCP connection in the partially open or closing phases must remain idle before the NAT considers the associated session a candidate for removal.

For more information, please refer to the *Personal Stateful Firewall Administration Guide.*

GGSN Features in Release 11.0

This section provides information for new features for the GGSN Service in Release 11.0.

Subscriber Session Trace Support

Subscriber-level Session Trace support adds one additional protocol on ASR 5000 or higher platform to support mobile users to connect to their enterprise networks through Generic Routing Encapsulation (GRE).

The Session Trace capability records and forwards all control activity for the monitored subscriber on the monitored interfaces. This is typically all the signaling and authentication/subscriber services messages that flow when a UE connects to the access network.

The UMTS network entities like SGSN and GGSN support 3GPP standards based session level trace capabilities to monitor all call control events on the respective monitored interfaces including Gn, Gi, Gx, and Gmb interface on GGSN. The trace can be initiated using multiple methods:

- Management initiation via direct CLI configuration
- Management initiation at AAA with trace activation via authentication response messages over Gx reference interface
- Signaling based activation through signaling from subscriber access terminal
- Once the trace is provisioned it can be provisioned through the access cloud via various signaling interfaces.

The session level trace function consists of trace activation followed by triggers. The time between the two events is treated much like Lawful Intercept where the UMTS network element buffers the trace activation instructions for the provisioned subscriber in memory using camp-on monitoring. Trace files for active calls are buffered as XML files using non-volatile memory on the local dual redundant hard drives on the ASR 5000 platforms. The Trace Depth defines the granularity of data to be traced. Six levels are defined including Maximum, Minimum and Medium with ability to configure additional levels based on vendor extensions.

IMPORTANT

Only Maximum Trace Depth is supported in the current release.

All call control activity for active and recorded sessions is sent to an off-line Trace Collection Entity (TCE) using a standards-based XML format over a FTP or secure FTP (SFTP) connection.

Note: In the current release the IPv4 interfaces are used to provide connectivity to the TCE. Trace activation is based on IMSI or IMEI.

The following figure shows a high-level overview of the session-trace functionality and deployment scenario:

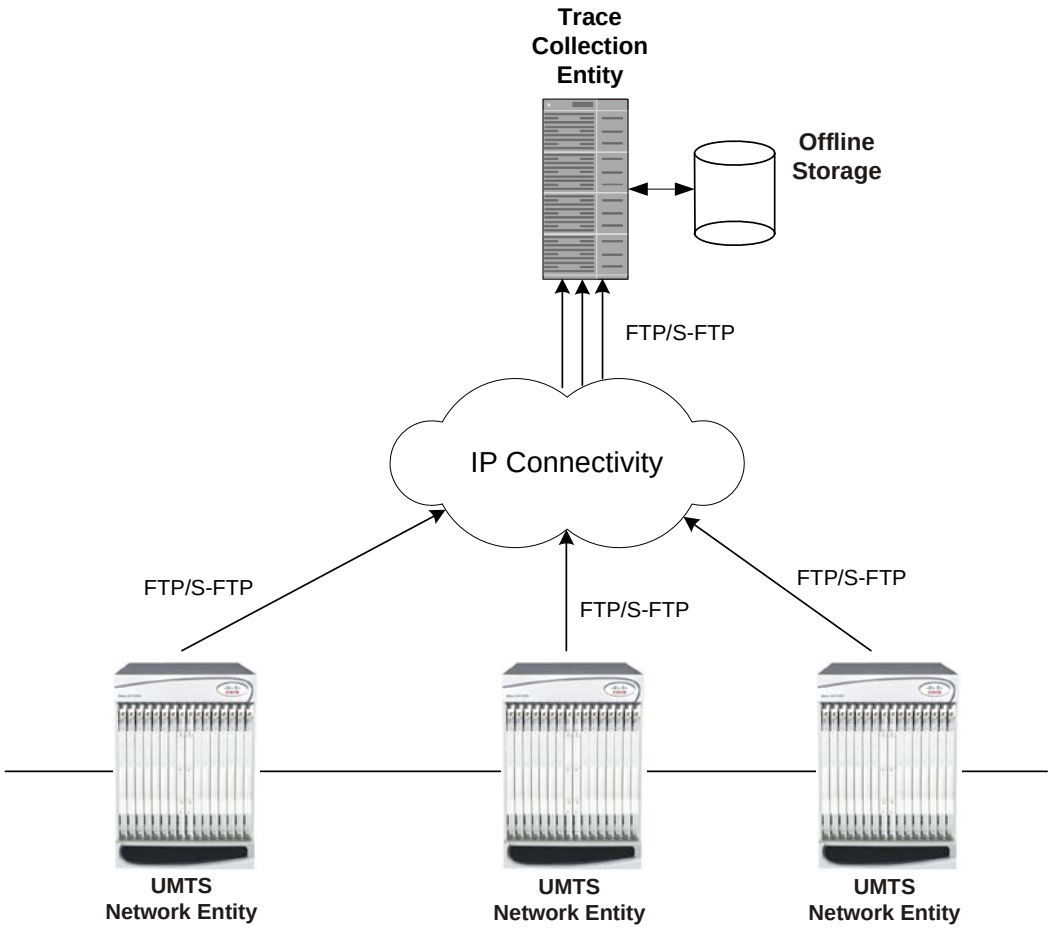

Figure 1-1 Session Trace Function and Interfaces

For more information on functioning and configuration of this interface, refer *GGSN Administration Guide*.

Framed-Route Attribute Support

The Framed-Route attribute provides routing information to be configured for the user on the network access server (NAS). The Framed-Route information will be returned from the RADIUS server in the Accounting Access-Accept message.

Mobile Router enables a router to create a PDP context which the GGSN authorizes using RADIUS server. The RADIUS server authenticates this router and includes a Framed-Route attribute in the access-accept response packet. Framed-Route attribute specifies the subnet routing information to be installed in the GGSN for the “mobile router.” If the GGSN receives a packet with a destination address matching the Framed-Route, the packet is forwarded to the mobile router through the associated PDP context.

How it Works

The process takes place in following way:

- The mobile router establishes an IP_PDU type context and is assigned an IP address as directed by the APN's configuration.
- The GGSN receives one or more Framed-Route RADIUS attribute(s) for the IP-PDU type in the RADIUS Access-Accept message.
- If a packet received by GGSN has the destination address matching one of the Framed-Route(s) assigned to the context or the mobile router's assigned IP address, it forwards the packet through the associated PDP context.

IMPORTANT

The IP address assigned to the mobile router need not be part of the Framed-Route(s) assigned to the context. For example, the mobile router may be assigned a private IP address while the Framed-Route may be a public IP subnet.

GnGp Handoff Support

In LTE deployments, the smooth handover support is required between 3G/2G and LTE networks, and Evolved Packet Core (EPC) is designed to be a common packet core for different access technologies. Since support for seamless handover across different access technologies is basic requirement for EPC, PGW needs to support handovers as user equipment (UE) moves across different access technologies.

Cisco's PGW supports inter-technology mobility handover between 4G and 3G/2G access. Interworking is supported between the 4G and 2G/3G SGSNs which provide only Gn and Gp interfaces but no S3, S4 or S5/S8 interfaces. Therefore these Gn/Gp SGSNs provide no functionality introduced specifically for the evolved packet system (EPS) or for interoperation with the E-UTRAN. These handovers are supported only with a GTP-based S5/S8 and PGW supports handoffs between GTPv2 based S5/S8 and GTPv1 based Gn/Gp tunneled connections. In this scenario, the PGW works as an IP anchor for the EPC.

IMPORTANT

Handover is supported for IPv4, IPv6 and IPv4/v6 PDN connections.

GnGp Handoff in Non-Roaming Scenario

Depending on the existing deployments, PLMN may operate Gn/Gp 2G and/or 3G SGSNs as well as MME and SGW for E-UTRAN access. In such cases, the PGW works as an anchor point for both GERAN/UTRAN and E-UTRAN access. Depending on APN, MME/SGSN select a PGW for each call.

In the home network (non-roaming) when UE firstly attaches to the E-UTRAN, it sets up a PDN connection with some EPS bearers and when the UE moves to Gn/Gp SGSN served GERAN/UTRAN access, handover is initiated from MME to the Gn/Gp SGSN. Gn/Gp SGSN then notifies PGW (with GGSN functionality) about the handoff of EPS bearers. During this handover, each EPS bearer in the PDN connection is converted into a PDP context.

The other way, when the UE first attaches on to Gn/Gp SGSN served GERAN/UTRAN, it sets up PDP contexts, and when the UE moves to E-UTRAN access, handover is initiated from Gn/Gp SGSN to the MME. MME then notifies the PGW (through SGW) about the handoff of PDP contexts to the E-UTRAN access. During this handover, all PDP contexts sharing the same APN and IP address are converted to EPS bearers of same PDN connection. Here one of the PDP context is selected as a Default bearer and rest of the PDP contexts are designated as Dedicated bearers.

GnGp Handoff in Roaming Scenario

In the roaming scenario, the vPLMN (Virtual PLMN) operates Gn/Gp 2G and/or 3G SGSNs as well as MME and SGW for E-UTRAN access and hPLMN (Home PLMN) operates a PGW. Other remaining things work as in non-roaming scenario.

MPLS Forwarding with LDP

Multi Protocol Label Switching (MPLS) is an operating scheme or a mechanism that is used to speed up the flow of traffic on a network by making better use of available network paths. It works with the routing protocols like BGP and OSPF and therefore it is not a routing protocol.

It generates a fixed-length label to attach or bind with the IP packet's header to control the flow and destination of data. The binding of the labels to the IP packets is done by the label distribution protocol (LDP). All the packets in a forwarding equivalence class (FEC) are forwarded by a label-switching router (LSR) which is also called an MPLS node. The LSR uses the LDP in order to signal its forwarding neighbors and distribute its labels for establishing a label switching path (LSP).

In order to support the increasing number of corporate APNs which have a number of different addressing models and requirements, MPLS is deployed to fulfill at least following two requirements:

- The corporate APN traffic must remain segregated from other APNs for security reasons.
- Overlapping of IP addresses in different APNs.

When deployed, MPLS backbone automatically negotiates the routes using the labels binded with the IP packets. Cisco GGSN as an LSR learns the default route from the connected provider edge (PE) while the PE populates its routing table with the routes provided by the GGSN.

GSS Features in Release 11.0

This section provides information for new GSS features for Release 11.0

None for this release.

HA Features in Release 11.0

This section provides information for new features in the Home Agent product in Release 11.0.

None for this release.

HSGW Features in Release 11.0

This section contains information on new 11.0 features that pertain to the HRPD Serving Gateway (HSGW) supporting eHRPD network services.

None for this release.

IP Services Gateway Features in Release 11.0

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

None for this release.

Mobility Management Entity Features in Release 11.0

This section contains information on features that pertain to the Mobility Management Entity (MME).

IMPORTANT

For more information about all of the features in this section, refer to the *Cisco ASR 5000 Series Mobility Management Entity Administration Guide*.

MME Operator Policy

The operator policy provides mechanisms to fine tune the behavior of subsets of subscribers above and beyond the behaviors described in the user profile. It also can be used to control the behavior of visiting subscribers in roaming scenarios, enforcing roaming agreements and providing a measure of local protection against foreign subscribers.

Load Balancing

The MME load balancing functionality permits UEs that are entering into an MME pool area to be directed to an appropriate MME in a manner that achieves load balancing between MMEs.

Mobility Restriction

Mobility Restriction comprises the functions for restrictions to mobility handling of a UE in E-UTRAN access. In ECM-CONNECTED state, the core network provides the radio network with a Handover Restriction List. The Handover Restriction List is used by the MME operator policy and specifies roaming, service area, and access restrictions. Mobility restrictions at the MME are defined in 3GPP TS 23.401.

Heuristic Paging

To limit the volume of unnecessary paging related signaling, the Cisco MME provides intelligent paging heuristics. Each MME maintains a list of “n” last heard from eNodeBs inside the TAI for the UE. The intent is to keep track of the eNodeBs that the AT commonly attaches to such as the cells located near a person's residence and place of work. During the average day, the typical worker spends the most time attaching to one of these two locations. When an incoming page arrives for the idle mode user, the MME attempts to page the user at the last heard from eNodeB. The MME uses Tracking Area Updates to build this local table. If no response is received within a configurable period, the MME attempts to page the user at the last “n” heard from eNodeBs. If the MME has still not received acknowledgement from the idle mode UE, only then does it flood the paging messages to all eNodeBs in the TAI.

IPv6 Transport (S1-MME)

The S1-MME interface service is supported on native IPv6. The Cisco MME service can run S1-AP/SCTP over IPv6 and support IPv6 addresses for S1-U endpoints.

SCTP Multi-homing (S1-MME)

The Cisco MME service supports up to two SCTP bind end point IPv4 or IPv6 addresses.

APN Restriction

The APN-Restriction value is defined in clause 15.4 of 3GPP TS 23.060. APN-Restriction affects multiple procedures, such as Initial Attach, TAU, PDN connectivity, and inter-MME handovers. The MME saves the APN-Restriction value received in create session response for an APN and uses the maximum of the values from the currently active PDNs in the next create session request. If a PDN is disconnected, then the maximum APN-Restriction is adjusted accordingly.

Inter-MME Handover (S10)

The MME now supports inter-MME handovers over the S10 reference point/interface. The S10 interfaces facilitates user mobility between two MMEs. It provides for the transfer of UE contexts from one MME to another using the GTPv2 protocol.

Serving Gateway Pooling Support

The S-GW supports independent service areas from MME pooling areas. Each cell is associated to a pool of MMEs and a pool of Serving GWs. Each cell is associated to a pool of MMEs and a pool of S-GWs. Once a cell selects an MME, that MME is able to select an S-GW which is in a S-GW pool supported by the cell.

Circuit Switched Fallback (SMS) Support Over SGs Interface

Circuit Switched Fall Back (CSFB) enables the UE to camp on an EUTRAN cell and originate or terminate voice calls through a forced switchover to the CS domain or other CS-domain services (e.g., Location Services (LCS) or supplementary services). Additionally, SMS delivery via the CS core network is realized without CSFB. Since LTE EPC networks were not meant to directly anchor CS connections, when any CS voice services are initiated, any PS based data activities on the EUTRAN network will be temporarily suspended (either the data transfer is suspended or the packet switched connection is handed over to the 2G/3G network).

Gn/Gp Handover between Pre-release 8 SGSNs

Enables an integrated EPC core network to anchor calls from multi-mode access terminals and support seamless mobility on call hand-offs between an LTE or GERAN/UTRAN access network. Provides a valuable function to enable LTE operators to generate incremental revenue from inbound roaming agreements with 2G/3G roaming partners.

MUR Features in Release 11.0

This section provides information for new features in the Mobility Unified Reporting (MUR) system in Release 11.0.

Bulkstats Schema Configuration Using GUI

In this release, the MUR GUI is used to configure bulk statistics schemas on gateway via SSH and SFTP. The associated reports can be viewed only when the schemas are configured.

IMPORTANT

Users with administrative privileges can only configure bulk statistics schemas on the gateway. In case the gateway is rebooted or SMC switchover occurs after the schema configuration is done, make sure the user reconfigures the bulk statistics schema.

For more information, please refer to the *Mobility Unified Reporting System Installation and Administration Guide* and *Mobility Unified Reporting System Online Help* documentation.

Busy Hour DPI Reports

This report provides the summary information of the hour at which the maximum fluctuation of a counter is observed. The Busy Hour (BH) is always determined in hour boundary.

- *Busy hour summary report based on date-range* - The busy hour is determined based on the date range.
- *Weekly busy hour report* - Weekly busy hour tables (sbi_bs_bh_weekly_data) are used to determine the busy hour for the specified week.
- *Monthly busy hour report* - Monthly busy hour tables (sbi_bs_bh_weekly_data) are used to determine busy hour for the specified month.

MUR implicitly detects BH in standard hour format, such as 03:00 to 04:00.

- BH Reporting is only available via the GUI (not in raw xls).
- BH Reports are calculated at the EOD.
- BH Reporting is only available under the DPI tab.
- BH radio button is available on the date panel.

- BH reporting is available for a date, date range, week and month.
- BH reporting is only available at the NOC level.
- BH Reports can be provided for the following (with dimensional filtering enabled):
  - Traffic analysis
  - Traffic distribution
  - Active flow counts
  - Unique subscriber hits per protocol

Clickstream Reporting

In this release, MUR allows user to create a “valid” regular expression for a referrer group. If the regular expression fails to find the referrer, the referrer is picked from the EDR record. If referrer field is absent, the record is mapped to the Default “None” referrer group. The regular expression is mapped over the “http-url” field of the EDR.

The user can also create one or more regular expressions for a domain group. If the regular expression fails to find the domain group, the record is mapped to the Default “Other” domain group. The regular expression is mapped over the “http-referrer” field of EDR record.

Data / File Purging Support

The MUR application supports purging any kind of aggregated data like half-hourly, daily, weekly, monthly, etc. This also supports purging of weekly summary table, monthly top N table, audit logs, etc.

MUR uses a python script, *purge_db.py*, to accomplish this task. This script runs daily at the end of the day, picks up the relevant tables, and then purges either data or archived files based on the configurations.

For more information, please refer to the *Mobility Unified Reporting System Installation and Administration Guide* and *Mobility Unified Reporting System Online Help* documentation.

Daily, Weekly and Monthly Aggregation for HTTP Reports

MUR now generates reports based on daily, weekly and monthly aggregated data so that the historical reports can be viewed even at a lowest granularity level.

Distribution of MUR Package File

In the MUR Software Releases prior to 11.0.100 build, this installation file is distributed with a .tar.gz extension. In the current release, this file is distributed in zip format.

Enhancements in Bulkstats Report

MUR now supports the following bulkstats summary reports:

- Performance Reports
  - Summary report based on date-range
  - Weekly performance report
  - Monthly summary report
- Busy Hour Reports - This report provides the summary information of the hour at which the maximum fluctuation of a counter is observed. The busy hour is always determined in hour boundary.
  - Busy hour summary report based on date-range
  - Weekly busy hour report
  - Monthly busy hour report
- Min/Max Reports - This report provides bulkstats data for the top 5 (max 5) or bottom 5 (min 5) list for the specified date/date-range.

Enhancements in HTTP TopN Reports

The following enhancements have been provided for TopN HTTP reports:

Content Type Aggregation

- TopN Content type report - Daily
- TopN Content type report - Weekly
- TopN Content type report - Monthly

HTTP Group Aggregation (Weekly/Monthly)

- TopN http group by Volume
- TopN http group by hit count
- TopN http group by unique subscriber hits

GUI reports for all above aggregation.

- Daily Report
- Date range report
- Weekly report
- Week range report
- Monthly report
- Month range report

MIB Support

In this release, MUR supports the basic SNMP alarms i.e. self-monitoring SNMP MIBs. For the complete list of supported MUR MIBs, see the *SNMP MIB Reference*.

Offline Subscriber Search Report

In this release MUR supports searching individual subscribers based on IMSI/MSISDN, and generates a subscriber-specific report showing the list of URLs visited by the subscriber, and other details like QoS, usage traffic, aggregate application/protocol breakdown, etc for the specified time period. MUR mainly supports this search functionality to track a subscriber or a set of subscribers for lawful intercept.

To use this Offline Reporting feature seamlessly, you must configure the EDR Filename Format appropriately through the Gateway configuration from ADMIN tab, and organize the archive directory date-wise. For information on how to manage the archive directory, see the *Managing Archive Directory* section in the *MUR Administration and Management* chapter of this guide.

For more information on this feature, see the *Mobility Unified Reporting System Online Help* documentation.

Support for Saved Queries

A "**Favourites**" button has been added to the GUI for Bulkstats and KPIs.

After selecting different filters for generating a report, the user clicks the "Favourites" button to save those selections. Saved queries\filters can be accessed through a selection list under the **FAVOURITES** tab.

Support for IPCF and HNB-GW Bulkstats

The following IPCF bulkstat schemas are now supported:

- pcc_policy_counter.xml
- pcc_quota_counter.xml
- pcc_service_counter.xml
- pcc_sp_endpt_counter.xml

The following HNB-GW bulkstat schemas are now supported:

- aal2_counter.xml
- alcap_counter.xml
- cs_nw_ranap_counter.xml
- cs_nw_rtp_counter.xml
- hnbgw_hnbap_counter.xml
- hnbgw_ranap_counter.xml
- hnbgw_rtp_counter.xml

- hnbgw_rua_counter.xml
- hnbgw_sctp_counter.xml
- ps_nw_ranap_counter.xml

NAT Features in Release 11.0

This section contains information for new features in the Network Address Translation (NAT) product in Release 11.0.

Flow Mapping Timer

The Flow Mapping timer is a new timer implemented as an extension to the existing idle-timeout in ECS, and is supported only for TCP and UDP flows. This flow mapping applies only for NAT enabled calls.

The purpose of this timer is to hold the resources such as NAT IP, NAT port, and Private IP NPU flow associated with a 5-tuple ECS flow until Mapping timeout expiry. If the feature is disabled, the Flow mapping timeout will not get triggered for TCP/UDP idle timed out flows. The resources such as NAT mapping will be released with the 5-tuple flow itself.

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

Session Recovery for SIP ALG

This release now supports session recovery for SIP ALG. Only one contact pinhole, and only one connected call and its associated media pinholes will be recovered for a subscriber. Any subscriptions, ongoing transactions, or unconnected calls will not be recovered. SIP ALG recovery data will be check-pointed using the variable length micro checkpointing mechanism.

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

NBR Attribute

A new NBR attribute **bearer 3gpp imsi** is added for NBR generation. This attribute provides the IMSI value of the subscriber.

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

Firewall-and-NAT Action

Firewall-and-NAT action is configured in the CLI Firewall-and-NAT Action Configuration Mode. It is now possible to enable/disable the check-pointing of NATed flows and control

the type of flows to be check pointed based on criteria. Check-pointing is done only for TCP and UDP flows.

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

PDG/TTG Features in Release 11.0

This section contains information about new features and functionality introduced in PDG/TTG in this release. For details, refer to *Cisco ASR 5000 Series Packet Data Gateway/Tunnel Termination Gateway Administration Guide.*

Support for Basic PDG Functionality

In addition to TTG functionality, this release supports the following PDG functionality:

- Tunnel creation and teardown
- APN configuration and statistics support
- RADIUS accounting
- DSCP marking
- Traffic policing and shaping
- DHCP proxy and DHCP relay support
- QoS negotiation
- Diameter reauthorization

AAA Mediation Accounting and Offline Charging

Offline charging is a process where charging information is collected at the same time as resource use. The charging information is then passed through a chain of charging functions. At the end of the process, CDR files are generated by the network, which are then transferred to the network operator's billing domain.

The charging trigger function (CTF) generates charging events and forwards them to the charging data function (CDF). The CDF, in turn, generates CDRs which are transferred to the charging gateway function (CGF). Finally, the CGF creates CDR files and forwards them to the billing domain. The CTF and CDF are integrated in the PDG, however, the CGF may exist as a separate entity or be integrated with the PDG. If the CGF is external to the PDG then the CDF forwards the CDRs to the CGF using the GTPP protocol.

In theASR5000, the PDG is integrated with the CTF and CDF and generates WLAN-CDRs based on triggered events over the Wz interface. The PDG offline charging involves the following functionalities for WLAN 3GPP IP access:

- Charging Trigger Function
- Charging Data Function
- Wz Reference Point

Storage of QoS Configuration Based on QCI

Traffic policing allows you to manage bandwidth usage on the network and limit bandwidth allowances to subscribers. QoS configurations are stored per QCI level (Quality of Service class identities.

Traffic policing enables the configuration and enforcement of bandwidth limitations on individual subscribers of a particular traffic class in a 3GPP service. Bandwidth enforcement is configured and enforced independently in the downlink and uplink directions.

PDIF Features in Release 11.0

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

None for this release.

PDSN Features in Release 11.0

This section provides information for new features in the Packet Data Serving Node in Release 11.0.

None for this release.

Peer-to-Peer Features in Release 11.0

This section provides information for new features in the inline Peer-to-Peer support.

P2P Protocols Detection Support

With release 11.0, the system supports the detection of the following P2P protocols:

- Armagettron
- Blackberry
- Citrix
- Clubpenguin
- Crossfire
- Facebook
- Fiesta
- Florensia
- Freenet
- Fring
- Funshion
- Guildwars

- Icecast
- ISAKMP
- Maplestory
- Meebo
- MGCP
- Octoshape
- PS3
- Real Media Stream
- Rfactor
- Shoutcast
- Splashfighter
- StealthNet
- Steam
- STUN
- TeamSpeak
- Thunder
- Tor
- Veoh TV
- WII
- Windows Media Stream
- World of Kungfu
- XDCC
- YourFreedom

The system also provides support for MSN video detection in release 11.0.

- MSN
  - Audio
  - Video
  - Non-audio/avideo

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

P-GW Features in Release 11.0

This section contains information on features that pertain to the Packet Data Network Gateway (P-GW).

IMPORTANT

For more information about all of the features in this section, refer to the *Cisco ASR 5000 Series Packet Data Network Gateway Administration Guide*.

DHCP Support

The P-GW supports dynamic IP address assignment to subscriber IP PDN contexts using the Dynamic Host Control Protocol (DHCP), as defined by the following standards:

- RFC 2131, Dynamic Host Configuration Protocol
- RFC 2132, DHCP Options and BOOTP Vendor Extensions

The method by which IP addresses are assigned to a PDN context is configured on an APN-by-APN basis. Each APN template dictates whether it will support static or dynamic addresses. Dynamically assigned IP addresses for subscriber PDN contexts can be assigned through the use of DHCP.

The P-GW acts as a DHCP server toward the UE and a DHCP client toward the external DHCP server. The DHCP server function and DHCP client function on the P-GW are completely independent of each other; one can exist without the other.

The P-GW does not support DHCP-relay.

IMPORTANT

Currently, the P-GW only supports DHCP with IPv4 addresses. IPv6 address support is planned at a later date.

Deferred IPv4 Address Allocation

Apart from obtaining IP addresses during initial access signalling, a UE can indicate via PCO options that it prefers to obtain IP address and related configuration via DHCP after default bearer has been established. This is also know as Deferred Address Allocation.

IPv4 addresses are becoming an increasingly scarce resource. Since 4G networks like LTE are always on, scarce resources such as IPv4 addresses cannot/should not be monopolized by UEs when they are in an ECM-IDLE state.

PDN-type IPv4v6 allows a dual stack implementing. The P-GW allocates an IPv6 address only by default for an IPv4v6 PDN type. The UE defers the allocation of IPv4 addresses based upon its needs, and relinquishes any IPv4 addresses to the global pool once it is done. The P-GW may employ any IPv4 address scheme (local pool or external DHCP server) when providing an IPv4 address on demand.

Direct Tunnel Support

Direct tunnel improves the user experience (e.g. expedited web page delivery, reduced round trip delay for conversational services, etc.) by eliminating S-GW tunnel “switching” latency from the user plane. An additional advantage of Direct Tunnel from an operational and capital expenditure perspective is that direct tunnel optimizes the usage of user plane resources by removing the requirement for user plane processing on the S-GW.

Gn/Gp GGSN/SGSN (GERAN/UTRAN)

The Cisco P-GW platform supports inter-technology mobility handover between E-UTRAN and GERAN/UTRAN, including interworking between the EPS and 3GPP 2G and/or 3G SGSNs, which provide only Gn and Gp interfaces but no S3, S4, or S5/S8 interfaces.

To allow this type of handover, the P-GW supports handoffs between GTPv2 based S5/S8 and GTPv1 based Gn/Gp tunneled connections; in other words, the P-GW supports GGSN (GPRS/UMTS anchor point) functionality. Handovers are supported for IPv4 and IPv6 PDN connections; there is no support of PDN type IPv4v6 as GGSN does not currently support PDP type IPv4v6.

IMPORTANT

To support the seamless handover of a session between GGSN and P-GW, the two independent services must be co-located on the same node and configured within the same context for optimum interoperation.

L2TP LAC Support

The system configured as a Layer 2 Tunneling Protocol Access Concentrator (LAC) enables communication with L2TP Network Servers (LNSs) for the establishment of secure Virtual Private Network (VPN) tunnels between the operator and a subscriber's corporate or home network.

Virtual APN Support

Virtual APNs allow differentiated services within a single APN.

The Virtual APN feature allows a carrier to use a single APN to configure differentiated services. The APN that is supplied by the MME is evaluated by the P-GW in conjunction with multiple configurable parameters. Then, the P-GW selects an APN configuration based on the supplied APN and those configurable parameters.

APN configuration dictates all aspects of a session at the P-GW. Different policies imply different APNS. After basic APN selection, however, internal re-selection can occur based on the following parameters:

- Service name
- Subscriber type
- MCC-MNC of IMSI
- Domain name part of username (user@domain)
- S-GW address

SCM Features in Release 11.0

This section provides information for new features in Release 11.0 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*.

None for this release.

Serving Gateway Features in Release 11.0

This section contains information on features that pertain to the Serving Gateway (S-GW).

IMPORTANT

For more information about all of the features in this section, refer to the *Cisco ASR 5000 Series Serving Gateway Administration Guide*.

IP Security (S1-U)

Enables network domain security for all IP packet switched LTE-EPC networks in order to provide confidentiality, integrity, authentication, and anti-replay protection. These capabilities are insured through use of cryptographic techniques.

The Cisco S-GW supports IKEv1 and IPSec encryption using IPv4 addressing. IPSec enables the following two use cases:

- Encryption of S8 sessions and EPS bearers in roaming applications where the P-GW is located in a separate administrative domain from the S-GW
- IPSec ESP security in accordance with 3GPP TS 33.210 is provided for S1 control plane, S1 bearer plane and S1 management plane traffic. Encryption of traffic over the S1 reference interface is desirable in cases where the EPC core operator leases radio capacity from a roaming partner's network.

S4 Interface Support

An SGSN can be upgraded to support 3GPP R8 S4-SGSN functions designed specifically to interconnect a GERAN/UTRAN access network to the EPC nodes. The S-GW includes the new S4 interface based on GTPv2-U protocol. The S4-SGSN facilitates soft hand-offs with the EPC network by providing control and mobility support between the inter-3GPP anchor function of the S-GW. The S4 reference interface provides user plane tunneling between the S-GW and 3GPP R8 SGSN in the event that direct tunneling is not used.

S12 Interface Support

S12 is a standards based reference interface defined in 3GPP TS 23.401. It enables inter-RAT handovers between EPC and UMTS access networks using direct tunnel procedures between the S-GW and an RNC in the 3G RAN. The S12 reference interface is loosely based on the standard Gn interface between gateway support nodes and as such it uses GTPv1-U tunneling.Conceptually similar to the direct tunneling procedures in 3G networks, the S12 optimizes the bearer plane by introducing single tunnels between the S-GW and RNC. This results in increased scalability and reduced latency.

SGSN Features in Release 11.0

This section provides information for new features in Release 11.0 for the Serving GPRS Support Node (SGSN). Additional information on these features can be found in the *SGSN Administration Guide*, and in the *CLI Reference Guide*.

Optimized Operator Policy

Description

The Operator Policy feature has been optimized for Release 11.0 with fewer lines of configuration needed because they are divided into reusable components.

The SGSN Operator Policy and SGSN APN Policy have been removed from the Global Configuration modes and their configuration commands have been divided between new configuration modes.

IMPORTANT

Existing Operator Policy configurations are not forward compatible to Release 11.0. All configurations for SGSNs, with operator policy-related configurations that were generated with software releases prior to Release 11.0, must be converted to enable them to operator with an SGSN running Release 11.0 or higher. Your Cisco Representative can accomplish this conversion for you.

New Configuration Modes

The old modes have been replaced with five new reusable-component (mix-and-match) configuration modes accessed through the Global Configuration mode:

APN-Profile Configuration Mode

An APN profile is a template which groups a set of APN-specific commands that may be applicable to one or more APNs. When a subscriber requests an APN that has been identified in a selected operator policy, then the set of commands in the associated APN profile will be applied.

APN Remap Table Configuration Mode

A remap table defines APN handling (for example: default APN, wildcard APN) and charging characteristics associated with a specific APN.

The commands in this new configuration mode implement the APN Aliasing feature.

Call-Control Profile Configuration Mode

A call-control profile can be used by the operator to fine-tune any desired restrictions or limitations needed to control call handling per subscriber or for a group of callers across IMSI ranges.

IMEI-Profile Configuration Mode

An IMEI profile group is a set of device-specific commands and parameters that control SGSN behavior when a Request is received from a device in the specified IMEI range.

The commands in this new configuration mode implement IMEI override (PR 119177) which is a new function in the optimized Operator Policy repertoire.

Operator Policy Configuration Mode

An operator policy associates APNs, APN profiles, an APN remap table, a call-control profile, and/or an IMEI profile to ranges of IMSIs (now defined under SGSN-Global configuration mode).

These profiles and tables are created and defined within their own configuration modes to generate sets of rules and instructions that can be reused and assigned to multiple policies. In this manner, an operator policy, as in earlier releases, manages the application of rules governing the services, facilities and privileges available to subscribers. These policies can override standard behaviors and provide mechanisms for an operator to get around the limitations of other infrastructure elements such as DNS servers and HLRs.

Configuration

1. Create an operator policy with the command in the Global Configuration mode.
2. Configure the IMSI range and associate it with a specific operator policy with commands in the SGSN-Global configuration mode. Note that this is a new command in the SGSN-Global mode.
3. Create (if needed) an APN profile with command in the Global Configuration mode.
4. Configure APN parameters with commands in the APN Profile configuration mode.
5. Create an APN remap table with the command in the Global Configuration mode.
6. Configuration APN handling/override and charging characteristics for the APN with commands in the APN Remap Table configuration mode. Note that APN handling/override is basically the major part of the enhanced APN Aliasing feature and now requires a license to use the commands for most APN handling/override functions.
7. Create a call-control profile with the command in the Global Configuration mode.
8. Configure call handling parameters with commands in the Call-Control Profile configuration mode.
9. Create (if needed) an IMEI profile with the command in the Global Configuration mode.
10. Configure device parameters with commands in the IMEI-Profile configuration mode.
11. Use commands in the Operator Policy configuration mode to associate all relevant profiles and remap tables with a specific operator policy.

IMPORTANT

APN profiles, Call-Control profiles, IMEI profiles, and APN remap tables are not valid until they are associated with one or more operator policies. An operator policy is not valid until an IMSI-range is associated with it.

For the up-to-date listing of configuration limits - for example, the maximum number of APN profiles that can be associated with an operator policy - see the *Engineering Rules* appendix in the ***SGSN Administration Guide***.

Expanded APN Profile Associations

With this MR release, the maximum number of APN profiles that can be associated with a single operator policy has been increased from 10 to 50. For details and other limits, refer to the *Engineering Rules* appendix in the ***SGSN Administration Guide***

Support for Narrowband SS7

Description

Prior to this release, the ASR 5000 SGSN only supported SS7 signaling links to the HLR via ATM-AAL5 broadband or IP (SIGTRAN) over Ethernet or ATM. With this release, the SGSN has fully implemented the MTP layer (in conformance with ITU Q701) to support high speed and low speed narrowband links via EI or T1.

Narrowband support is provided across these interfaces:

- Gr Interface (HLR)
- Gs Interface (MSC/VLR)
- Gf Interface (EIR)
- Gd Interface (SMS-C)

Configuration

Narrowband SS7 links are configured as part of the SS7 routing domains as individual links within a linkset. The link configuration requires the operator to specify either high speed or low speed narrowband.

For descriptions of the CLI commands used to configure narrowband SS7 links, refer to the to the *SGSN Administration Guide* and the *Command Line Interface Reference*.

IMPORTANT

Currently, this feature is only available for the 'china' routing domain variant.

APN Aliasing and Licensing

Description

In many situations, the APN provided in the Activation Request is unacceptable - perhaps it does not match with any of the subscribed APNs or it is misspelled - and would result in the SGSN rejecting the Activation Request.

The APN Aliasing feature enables the operator to override an incoming APN - specified by a subscriber or provided during the APN selection procedure (TS 23.060) - or replace a missing APN with an operator-preferred APN.

The APN Aliasing feature provides a set of override functions: Default APN, Blank APN, APN Remapping, and Wildcard APN to facilitate such actions as:

- overriding an HFL-mismatched APN with a default APN.
- overriding an APN on the basis of charging characteristics.
- overriding an APN by replacing part or all of the network or operator identifier with information defined by the operator - for example, MNC123.MCC456.GPRS >> MNC222.MCC333.GPRS.
- overriding an APN for specific subscribers (based on IMSI) or for specific devices (based on IMEI).

Configuration

Configuration for all of the functions of the APN Aliasing feature is accomplished in the APN Remap Table configuration mode of the Operator Policy Feature.

APN Aliasing is implemented on the basis of the APN profile(s) and/or IMEI profile(s) configured and associated with one or more operator policies.

Unless the APN remap table is associated with an APN profile and/or an IMEI profile and an operator policy then the remap table is invalid and the APN Aliasing overrides will not occur.

IMPORTANT

With Release 11.0, all functions that are a part of the APN Aliasing feature, except the Wildcard APN function, require the APN Aliasing license (600-00-7626).

For CLI command details, refer to the *Command Line Interface Reference* and the *SGSN Administration Guide*.

Iu Redundancy (ECMP over ATM)

Description

Iu Redundancy is the ASR 5000's implementation of equal-cost multi-path routing (ECMP) over ATM. It is based on the standard ECMP multi-path principle of providing multiple next-hop-routes of equal cost to a single destination for packet transmission. ECMP works with most routing protocols and can provide increased bandwidth when traffic load-balancing is implemented over multiple paths.

ECMP over ATM will create an ATM ECMP group when multiple routes with different destination ATM interfaces are defined for the same destination IP address. When transmitting a packet with ECMP, the NPU performs a hash on the packet header being transmitted and uses the result of the hash to index into a table of next hops. The NPU looks up the ARP index in the ARP table (the ARP table contains the next-hop and egress interfaces) to determine the next-hop and interface for sending packets.

Configuration

ECMP over ATM is configured in the same way that a single Iu (ATM) route has been defined,

1. Within the appropriate context, use the ip route and interface commands in the Context Configuration mode.
2. Use the PVC configuration mode and the Port ATM configuration mode to define and bind the PVC.
3. Repeat to add multiple routes.

The difference between an ATM ECMP and a traditional Ethernet ECMP - an ATM ECMP group is automatically generated when multiple routes with different destination ATM interfaces are defined for the same destination IP address.

None of the commands are new. For configuration CLI details refer to the *Command Line Interface Reference* and the *SGSN Administration Guide*.

Verify Configuration

Display the configured IP routes:

```
[one]asr5000# show ip route
"*" indicates the Best or Used route.

Destination         Nexthop          Protocol   Prec Cost Interface
*1.1.1.0/24          0.0.0.0         static     1    0    31/1-100-100
*1.1.1.0/24          0.0.0.0         static     1    0    31/2-100-100
*172.10.10.0/24      0.0.0.0         connected  0    0    31/1-100-100
*172.10.11.0/24      0.0.0.0         connected  0    0    31/2-100-100


Total route count : 4
Unique route count: 3
Connected: 2 Static: 2
```

CAMEL Service Phase 3, Ge Interface

Description

The ASR 5000 SGSN provides PDP session support as defined by Customized Applications for Mobile network Enhanced Logic (CAMEL) phase 3.

CAMEL service enables operators of 2.5G/3G networks to provide operator-specific services (such as prepaid GPRS service and prepaid SMS service) to subscribers, even when the subscribers are roaming outside their HPLMN.

At this time, the ASR 5000 SGSN supports the following GPRS-related functionality in CAMEL phase 3:

- Control of GPRS PDP contexts

Functional support for CAMEL interaction includes:

- PDP Context procedures per 3GPP TS 29.002
  - GPRS TDP (trigger detection point) functions
  - default handling codes, if no response received from SCP
  - GPRS EDP (event detection points) associated with SCP
  - Charging Procedures: Handle Apply Charging GPRS & Handle Apply Charging Report GPRS
- “GPRS Dialogue scenario 2" for CAMEL control with SCP
- CAMEL-related data items in an S-CDR:
  - SCF Address
  - Service Key
  - Default Transaction Handling
  - Level of CAMEL service (phase 3)
- Session Recovery for all calls that have an established CAMEL association.

Ge Interface

The ASR 5000 implementation of CAMEL uses standard CAP protocol over a Ge interface between the SGSN and the SCP. This interface can be deployed over SS7 or SIGTAN.

The SGSN's Ge support includes use of the gprsSSF CAMEL component with the SGSN and the gsmSCF component with the SCP.

CAMEL Configuration

To provide the CAMEL interface on the SGSN, a new service configuration mode, called "CAMEL Service", has been introduced on the SGSN.

1. An SCCP Network configuration must be created or exist already.
2. A CAMEL Service instance must be created.
3. The CAMEL Service instance must be associated with either the SGSN Service configuration or the GPRS Service configuration in order to enable use of the CAMEL interface.

4 The CAMEL Service must be associated with the SCCP Network configuration.

Until a CAMEL Service is properly configured, the SGSN will not process any TDP for pdp-context or mo-sms.

For configuration CLI details, refer to the *SGSN Administration Guide* and the *Command Line Interface Reference*.

Inter-Card APS for SGSN Channelized Line Cards

Description

Automatic Protection Switching (APS) is now available on an inter-card basis for SONET configured CLC2 line cards. Multiple Switching Protection (MSP) is available for SDH configured CLC2 line cards.

APS offers superior redundancy for SONET/SDH equipment and supports recovery from card failures and fiber cuts. APS allows an operator to configure a pair of SONET lines for line redundancy. In the event of a fiber cut, the active line switches automatically to the standby line within 60 milliseconds (10 millisecond initiation and 50 millisecond switchover).

The protection mechanism used for the APS is from the port on the active card to the port on the standby card. The connection is unidirectional.

Configuration

In the Card Configuration Mode, APS is enabled with the **`redundancy`** command.

Behavioral Changes

APN Aliasing Requires License

As of Release 11.0, all the functions associated with the new APN Aliasing feature, except **`wildcard-apn`**, require the APN Aliasing license 600-00-7626. This feature set is typically configured in the new Operator Policy features in the APN Remap Table configuration mode.

SGSN Commands Added to SSD Command

When **`show support details`** is issued on an SGSN, outputs from the following commands will be included in the report:

- show bssap+ statistics verbose
- show bssgp statistics verbose
- show global-title-translation address-map all
- show global-title-translation association all
- show gprs-service all
- show gprsns statistics sns-msg-stats
- show gs-service all

- show call-control profile all
- show apn-profile all
- show imei-profile all
- show iups-service all
- show llc statistics verbose
- show map-service all
- show network-service-entity fr-config
- show sgsn sessmgr all memory statistics
- show operator-policy all
- show sgsn-service all
- show sgtp-service all
- show sndcp statistics verbose
- show tcap statistics
- show map statistics
- show sms statistics

PDP Context Preservation

Previously, PDP preservation was not supported for 2G and for active PDP context with conversational/streaming traffic classes.

1. The SGSN was not downgrading the maximum bitrates to zero.
2. The SGSN was not updating the GGSN on receiving Radio Status or Suspend from the BSCs, and if Radio Status or Suspend was received while waiting for Modify Accept from the MS (during network-initiated PDP context modification), then the PDP contexts were deactivated.

Now, PDP preservation is supported. Upon receiving Radio Status or Suspend from a BSC, the maximum bitrates (MBR) will be downgraded to zero and the GGSN will be updated with the modified MBR.

Disassociating GTP from SM/PMM

In some cases, PMM and SM layers need to abort a session before their state machines become too complex. In such scenarios, PMM and SM inform the GTP layer to purge any GTP tunnels associated with the session. Currently, the GTP layer just sends a Delete PDP Context (DPC) request to the GGSN and frees the tunnel immediately.

Now, the GTP layer maintains the tunnel in a disassociated fashion until a DPC response is received or the request times-out. In cases where a new GTP tunnel needs to be created and there is no free tunnel available, the SGSN aborts the oldest disassociated tunnel and uses it for the new requirement.

Disassociated tunnel statistics are tracked in the **`show sgtpc statistics verbose`** command.

Gb/IP Scaling Requirements

The SGSN now supports the following capacities for the Gb-over-IP interface:.

- 2048 NSEIs
- 2500 NSEs per RA
- No limit to the number of NSEs sharing the same RA
- NSVCs per NSE
  - FR = 128
  - IP = 128 X 4
- Number of BVCs per SGSN per NSE - 64,000

IMPORTANT

Do not configure bulkstats if 2,500 RAs are configured on the SGSN.

GPRS Scaling Requirements

The SGSN now supports the following capacities for the GPRS service.

- 2048 NSEIs
- 2500 RAs per NSE
- No limit to the number of NSEs sharing the same RA
- NSVCs per NSE
  - FR = 128
  - IP = 128 X 4
- Number of BVCs per SGSN per NSE - 64,000

IMPORTANT

Do not configure bulkstats if 2,500 RAs are configured on the SGSN.

show port utilization table

The output of the show port utilization table command always displays zeros (0) when this command is issued for a CLC2 configured for service-type MTP2. This is a hardware issue.

Lawful Intercept Provisions

The maximum limit for LI provisions for this release is 20,000.

Web Element Manager Features in Release 11.0

This section provides information for new features for the Web Element Manager application in Release 11.0.

Enhanced Load Configuration Feature

WEM's Load Configuration feature now enables users to manage all aspects of configuration file updates for systems that are accessed by an instance of the WEM.

The Load Configuration feature's user interface utilizes the structure and syntax of the ASR 5000 Command Line Interface (CLI) to provide users with the capability to efficiently duplicate, edit, create, and save configuration files and templates. Configuration files can be applied to one or more ASR 5000s. Configuration templates also can be created or edited to quickly apply updates to selected systems.

For more information on the Enhanced Load Configuration feature, refer to the *Configuration Management* chapter in this document.

Support for Viewing SSC Alarm and Bulkstat Information

WEM now supports the viewing of alarm and bulkstat information for a specified Cisco Subscriber Service Controller (SSC).

For more information on SSC support in WEM, refer to the *Accounting Management* chapter in this document.

CHAPTER 2
FAULT MANAGEMENT

This section contains additions and changes made to the fault management features available in Release 11.0:

SNMP MIB Objects in Release 11.0

This section lists the MIB objects and alarms new / modified in Release 11.0.

New Objects

- starIPPoolGroupTable
- starIPPoolGroupEntry
- starIPPoolGroupVpnID
- starIPPoolGroupID
- starIPPoolGroupName
- starIPPoolGroupVpnName
- starIPPoolGroupUsed
- starIPPoolGroupHold
- starIPPoolGroupRelease
- starIPPoolGroupFree
- starIPPoolGroupPctUsed
- starIPPoolGroupAvail
- starSPRServerIpAddr
- starEPDGServiceStart
- starEPDGServiceStop
- starHNBGWSGSNRanapReset
- starHNBGWMSCRanapReset
- starALCAPNodeReset
- starALCAPPathReset
- starALCAPPathBlock
- starALCAPPathUnBlock
- starPCCPolicyServiceStart
- starPCCPolicyServiceStop
- starPCCQuotaServiceStart
- starPCCQuotaServiceStop
- starPCCAFServiceStart
- starPCCAFServiceStop
- starThreshPCCPolicySessions
- starThreshClearPCCPolicySessions
- starThreshPerServicePCCPolicySessions
- starThreshClearPerServicePCCPolicySessions
- starThreshPCCQuotaSessions
- starThreshClearPCCQuotaSessions

- starThreshPerServicePCCQuotaSessions
- starThreshClearPerServicePCCQuotaSessions
- starThreshPCCAFSessions
- starThreshClearPCCAFSessions
- starThreshPerServicePCCAFSessions
- starThreshClearPerServicePCCAFSessions
- starThreshHNBGWHnbSess
- starThreshClearHNBGWHnbSess
- starThreshHNBGWUeSess
- starThreshClearHNBGWUeSess
- starThreshHNBGWIuSess
- starThreshClearHNBGWIuSess
- starThreshPerServicePDGSessions
- starThreshClearPerServicePDGSessions
- starThreshSystemCapacity
- starThreshClearSystemCapacity
- starThreshTpoRtoTimeout
- starThreshClearTpoRtoTimeout
- starThreshTpoDnsFailure
- starThreshClearTpoDnsFailure
- starThreshTpoLowCompressionGain
- starThreshClearTpoLowCompressionGain
- starGPRSServiceStart
- starGPRSServiceStop
- starGPRSNseDown
- starGPRSNseUp
- starGPRSNsvcDown
- starGPRSNsvcUp
- starGPRSBvcDown
- starGPRSBvcUp
- starSDHE1TribDown
- starSDHE1TribUp
- starSDHFractE1LMIDown
- starSDHFractE1LMIUp
- starPHSPCServiceStart
- starPHSPCServiceStop
- starSDHLopDown
- starSDHLopUp

- starPHSGWServiceStart
- starPHSGWServiceStop
- starCSCFPeerServerName
- starIPMSServerEntry
- starHNBGWServTable
- starHNBGWSerVpnID
- starHNBGWSerSvcID
- starSessHNBGWVpnName
- starSessHNBGWServName
- starSessHNBGWCsNwName
- starSessHNBGWPsNwName
- starSessHNBGWSgsnPtCd
- starSessHNBGWMscPtCd
- starPCFTable
- starPCFEntry
- starPCFSvcID
- starPCFIpAddr
- starPCFVpnID
- starPCFVpnName
- starPCFServName
- starPCFRrqRcvd
- starPCFRrqAccepted
- starPCFRrqDenied
- starPCFRrqDiscarded
- starPCFInitialRrqRcvd
- starPCFInitialRrqAccepted
- starPCFIntraPDSNActiveHORrqAccepted
- starPCFIntraPDSNDormantHORrqAccepted
- starPCFInterPDSNHORrqAccepted
- starPCFInitialRrqDenied
- starPCFInitialRrqDiscarded
- starPCFRenewRrqRcvd
- starPCFRenewRrqAccepted
- starPCFRenewActiveRrqAccepted
- starPCFRenewDormantRrqAccepted
- starPCFRenewRrqDenied
- starPCFRenewRrqDiscarded
- starPCFDeregRrqRcvd

- starPCFDeregRrqAccepted
- starPCFDeregDormantRrqAccepted
- starPCFDeregRrqDenied
- starPCFDeregRrqDiscarded
- starPCFIntraPDSNActiveAnidHORrqAccepted
- starPCFIntraPDSNDormantAnidHORrqAccepted
- starPCFDeniedUnSpeReason
- starPCFDeniedAdmProh
- starPCFDeniedInsufResource
- starPCFDeniedMobNodeAuthFail
- starPCFDeniedIdentMismatch
- starPCFDeniedPoorFormedReq
- starPCFDeniedUnknownPDSNAddr
- starPCFDeniedRevTunnelUnavail
- starPCFDeniedRevTunnelRequire
- starPCFDeniedUnrecogVendorId
- starPCFDeniedSessionClosed
- starPCFDeniedBsnSessionInfoUnavail
- starPCFegUpdTransmitted
- starPCFRegUpdAccepted
- starPCFRegUpdateRpLifetimeExpiry
- starPCFRegUpdateUpperLayerIntiated
- starPCFRegUpdateOtherReason
- starPCFRegUpdateHORelease
- starPCFRegUpdateSessmgrDied
- starPCFAuxA10ConnectionsSetup
- starPCFSessionsDenied
- starPCFSessionsInit
- starPCFSessionsReneg
- starPCFDiscLcpRemote
- starPCFDiscRpRemote
- starPCFDiscRpLocal
- starPCFDiscMaxIpcpRetr
- starPCFDiscMaxIpv6cpRetr
- starPCFDiscMaxLcpRetr
- starPCFDiscAuthFail
- starPCFDiscSessSetupTimeout
- starPCFDiscFlowAddFail

- starPCFDiscInvDestContext
- starPCFDiscLcpOptFail
- starPCFDiscIpcpOptFail
- starPCFDiscIpv6cpOptFail
- starPCFDiscNoRemIpAddr
- starPCFDiscDetectionFail
- starPCFDiscMisc
- starPCFCurrentSessions
- starPCFSessionsSetup
- starPCFSessionsRelsese
- starPCFCurrentRevaSessions
- starPCFRevaSessionsSetup
- starPCFRevaSessionsRelsese
- starSPRServerUnreachable
- starSPRServerReachable
- starRP1xTxBytes
- starRPDiscMisc
- starRP1xTxPackets
- starRP1xRxPackets
- starRPDoTxBytes
- starRPDoRxBytes
- starRPDoTxPackets
- starRPDoRxPackets
- starALCAPServTable
- starALCAPSerEntry
- starALCAPSerVpnID
- starALCAPSerSvcID
- starSessALCAPVpnName
- starSessALCAPServName
- starSessALCAPAAL2NodeName
- starSessALCAPPathId
- starMMES1AssocTable
- starMMES1AssocEntry
- starMMES1AssocSvcID
- starMMES1AssocENBID
- starMMES1AssocVpnName
- starMMES1AssocServName

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 11.0. Topics covered in this chapter are:

New Configuration Commands

This section contains configuration commands that are new in Release 11.0. New commands in this version are divided into the following sections:

- *Common Commands - New in Release 11.0*
- *ASN GW Commands - New in Release 11.0*
- *Content Filtering Commands - New in Release 11.0*
- *ECS Commands - New in Release 11.0*
- *Firewall Commands - New in Release 11.0*
- *GGSN Commands - New in Release 11.0*
- *HA Commands - New in Release 11.0*
- *Mobility Management Entity Commands - New in Release 11.0*
- *NAT Commands - New in Release 11.0*
- *Packet Data Network Gateway Commands - New in Release 11.0*
- *PDIF Commands - New in Release 11.0*
- *PDSN Commands - New in Release 11.0*
- *Peer-to-Peer - New in Release 11.0*
- *Serving Gateway Commands - New in Release 11.0*
- *Session Control Manager Commands - New in Release 11.0*
- *SGSN Commands - New in Release 11.0*

Common Commands - New in Release 11.0

This section provides information on new commands that are common to products in Release 11.0.

diameter dynamic-rules request-quota

This command enables to request quota immediately in the CCR sent to Gy interface when the traffic matches the dynamic rules with Online AVP enabled and received over Gx interface.

CLI (Credit Control Configuration Mode)

`diameter dynamic-rules request-quota { on-traffic-match | on-receiving-rule }`

`default diameter dynamic-rules request-quota`

Web Element Manager Path

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

event-report-indication

This command enables event report indication.

CLI (Policy Control Configuration Mode)

`[ default | no ] event-report-indication { all | pgw-trace-control | qos-change | rai-change | rat-change | sgsn-change | ue-timezone-change | user-loc-change } [ pgw-trace-control ] [ qos-change ] [ rai-change ] [ rat-change ] [ sgsn-change ] [ ue-timezone-change ] [ user-loc-change ]`

Web Element Manager Path

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

mediation-device

This command enables the use of a mediation device for PDG-TTG subscriber and specifies the system context to use for communicating with the device.

CLI (Subscriber Configuration Mode)

`[ no | default ] mediation-device context-name` *`<context-name>`* **`[ no-interims ]`**

Web Element Manager Path

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

mpls-ip

This command globally enables the MPLS forwarding of IPv4 packets along normally routed paths.

CLI (Context Configuration Mode)

`[ no ] mpls-ip`

Web Element Manager Path

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

radius trigger

This command enables RADIUS triggers.

CLI (AAA Group Configuration & Context Configuration Modes)

`[ no ] radius trigger { ms-timezone-change | qos-change | rai-change | rat-change | serving-node-change | uli-change }`

Web Element Manager Path

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

show mpls ldp

This command is used to display the statistical information on Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) configuration.

CLI (Exec Mode)

`show mpls ldp { bindings { ldp-id` *`IPv4_add`* **`| local [ ldp-id | local | prefix | remote ] | prefix`** *`IPv4_addr`* **`| remote } | discovery | neighbor { detail | ldp-id } }`**

Web Element Manager Path

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

show support details

The new keyword – **`compress`** – enables the operator to generate a compressed .tar.gz file for the output of the **`show support details to file`** command.

CLI (Exec Mode)

`show support details [ to file url  [ compress ] ]`

`show mpls ldp { bindings { ldp-id` *`IPv4_add`* **`| local [ ldp-id | local | prefix | remote ] | prefix`** *`IPv4_addr`* **`| remote } | discovery | neighbor { detail | ldp-id } }`**

Web Element Manager Path

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

ASN GW Commands - New in Release 11.0

None for this release.

Content Filtering Commands - New in Release 11.0

This section provides information on new CF commands available in Release 11.0.

deny-response code

This command configures the deny response message that is to be sent from ICAP server to the subscribers.

CLI (Content Filtering Server Group Configuration Mode)

deny-response code { 200 message *string* **| 403 }**

{ default | no } deny-response code

Web Element Manager Path

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

ECS Commands - New in Release 11.0

None for this release.

Firewall Commands - New in Release 11.0

This section provides information on new commands available in Release 11.0.

firewall icmp-echo-id-zero

This command configures Stateful Firewall action on echo packets with ICMP ID zero.

CLI (Firewall-and-NAT Policy Configuration Mode)

firewall icmp-echo-id-zero { drop | permit }
default firewall icmp-echo-id-zero

Web Element Manager Path

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

firewall tcp-partial-connection-timeout

This command configures action on idle timeout for partially open connections.

CLI (Firewall-and-NAT Policy Configuration Mode)

firewall tcp-partial-connection-timeout *timeout*

{ default | no } tcp-partial-connection-timeout

Web Element Manager Path

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

GGSN Commands - New in Release 11.0

This section provides information on new commands available in Release 11.0.

associate pgw-service

This command enables a previously configured P-GW service to which handover will be done by the GGSN service. The P-GW service must be configured in the context configuration mode before using this configuration.

CLI (GGSN Service Configuration Mode)

associate pgw-service *svc_name*

no associate pgw-service

Web Element Manager Path

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

trace-collection-entity

New command added to configure the Trace Collection Entity for subscriber-level session support in GGSN service configuration mode.

CLI (GGSN Service Configuration Mode)

trace-collection-entity *tce_ip_addr*

no trace-collection-entity

Web Element Manager Path

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

HA Commands - New in Release 11.0

None for this release.

Mobility Management Entity Commands - New in Release 11.0

This section provides information on new Mobility Management Entity (MME) commands available in Release 11.0.

apn

This command identifies an APN (access point name) and associates it with an APN profile (created separately in the APN Profile configuration mode).

CLI (Operator Policy Configuration Mode)

apn { default-apn-profile *apn_profile_name* **| network-identifier** *apn_net_id* **apn-profile** *apn_profile_name* **| operator-identifier** *apn_op_id* **apn-profile** *apn_profile_name* **}**

Web Element Manager Path

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

apn-profile

Creates an instance of an APN profile.

CLI (Global Configuration Mode)

[no] apn-profile *apn_profile_name*

Web Element Manager Path

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

apn-remap-table

Creates an instance of an APN remap table.

CLI (Global Configuration Mode)

[no] apn-remap-table *apn_remap_table_name*

Web Element Manager Path

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

associate

This command associates various MME-specific lists and databases with this call-control profile.

CLI (Call Control Profile Configuration Mode)

associate { ho-restrict-list *list_name* **| hss-peer-service** *service_name* **[s13-interface | s6a-interface] | tai-mgmt-db** *tai-db_name* **}**

Web Element Manager Path

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

associate

Associate an APN remap table and a call-control profile with the operator policy.

CLI (Operator Policy Configuration Mode)

`associate { apn-remap-table` *`table_id`* **`| call-control-profile`** *`profile_id`* **`}`**

Web Element Manager Path

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

attach

This command defines attach-related configuration for this call-control profile.

CLI (Call Control Profile Configuration Mode)

`attach access-type { gprs | umts } { all | location-area-list instance` *`list_id`* **`} { failure-code`** *`code`* **`| user-device-release { before-r99 failure code`** *`code`* **`| r99-or-later failure code`** *`code`* **`}`**

Web Element Manager Path

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

authenticate

This command enables/disables authentication for procedures, such as Attach and Service Request.

CLI (Call Control Profile Configuration Mode)

`[ no ] authenticate { activate | all-events | attach | detach | rau | service-request | tau }`

Web Element Manager Path

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

auth-request

Configures the number of authentication vectors the MME requests in an Authentication-Information-Request (AIR) message to the HSS for each UE requiring authentication.

CLI (HSS Peer Service Configuration Mode)

`auth-request num-auth-vectors` *`num`*

Web Element Manager Path

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

bind

Binds the service to a logical IP interface serving as the SGs interface.

CLI (MME SGs Service Configuration Mode)

bind ipv4-address *ip_address*

Web Element Manager Path

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

call-control-profile

Creates an instance of a call-control profile.

CLI (Global Configuration Mode)

[no] call-control-profile *cc_profile_name*

Web Element Manager Path

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

description

Define a descriptive string relevant to the specific APN profile.

CLI (APN Profile Configuration Mode)

description *description*

Web Element Manager Path

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

description

Define a string that describes the particular APN remap table.

CLI (APN Remap Table Configuration Mode)

description *description*

Web Element Manager Path

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

description

Set to a relevant descriptive string.

CLI (Call Control Profile Configuration Mode)

description *description*

Web Element Manager Path

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

description

Set to a relevant descriptive string.

CLI (Operator Policy Configuration Mode)

`description` *`description`*

Web Element Manager Path

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

diameter hss-dictionary

Specifies the Diameter Credit Control dictionary for the HSS peer service.

CLI (HSS Peer Service Configuration Mode)

`diameter hss-dictionary { custom1 | standard }`

Web Element Manager Path

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

diameter hss-endpoint

This commands associates a preconfigured Diameter origin endpoint with this HSS peer service.

CLI (HSS Peer Service Configuration Mode)

`diameter hss-endpoint` *`endpoint_name`* **`[ eir-endpoint`** *`eir_endpoint_name`* **`]`**

Web Element Manager Path

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

dns-pgw

Define the context to be used to do DNS lookup for P-GWs

CLI (Call Control Profile Configuration Mode)

`[ remove ] dns-pgw context` *`ctxt_name`*

Web Element Manager Path

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

dns-sgw

Define the context to be used to do DNS lookup for S-GWs.

CLI (Call Control Profile Configuration Mode)

`[ remove ] dns-sgw context` *`ctxt_name`*

Web Element Manager Path

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

dynamic-peer-discovery

Configures the system to dynamically locate peer Diameter servers by means of DNS.

CLI (Diameter Endpoint Configuration Mode)

dynamic-peer-discovery [protocol { sctp | tcp }]

Web Element Manager Path

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

dynamic-peer-realm

Configures the name of the realm where peer Diameter servers can be dynamically discovered.

CLI (Diameter Endpoint Configuration Mode)

[no] dynamic-peer-realm *realm_name*

Web Element Manager Path

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

encryption-algorithm-lte

Define the priorities for using the encryption algorithms.

CLI (Call Control Profile Configuration Mode)

encryption-algorithm-lte priority1 128-eea { 0 | 1 | 2 } priority2 128-eea { 0 | 1 | 2 } priority3 128-eea { 0 | 1 | 2 }

Web Element Manager Path

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

equivalent-plmn

Configures the definition for an equivalent PLMNID and the preferred radio access technology (RAT).

CLI (Call Control Profile Configuration Mode)

equivalent-plmn radio_access_technology { 2G | 3g | 4g | any } plmnid mcc *mcc_number mnc_number* **priority** *priority*

Web Element Manager Path

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

forbidden

Configures the handover restriction lists provided to eNodeBs where handover restrictions are enforced for UEs.

CLI (MME Handover Restriction List Configuration Mode)

[no] forbidden { inter-rat { all | cdma2000 | geran | utran } | location-area plmnid *id* | tracking-area plmnid *id* }

Web Element Manager Path

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

gtpv2

Configures GTPv2 piggybacking support from the MME to the P-GW. A piggybacking flag is sent by the MME to a PGW in the S11 “Create Session Request” message and determines whether dedicated bearer creation (Create Bearer Request) is piggybacked onto the “Create Session Response” message or not.

CLI (MME Service Configuration Mode)

[default | no] gtpv2 piggybacking

Web Element Manager Path

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

gw-selection

This command configuration the parameters controlling the gateway selection process.

CLI (Call Control Profile Configuration Mode)

[remove] gw-selection { co-location | pgw weight | sgw weight | topology }

Web Element Manager Path

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

hash-value

Configures the Visitor Location Register hash value mapping for this pool area.

CLI (MME LAC Pool Area Configuration Mode)

hash-value { *value* | non-configured-values | range *value* to *value* } use-vlr *vlr_name*

Web Element Manager Path

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

ho-restrict-list

Creates a handover (HO) restriction list or specifies an existing HO restriction list and enters the Handover Restriction List Configuration Mode.

CLI (MME Policy Configuration Mode)

[no] ho-restrict-list *list_name* **[-noconfirm]**

Web Element Manager Path

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

hss-peer-service

Creates a Home Subscriber Service (HSS) peer service or configures an existing HSS peer service and enters the HSS Peer Service Configuration Mode.

CLI (Context Configuration Mode)

hss-peer-service *service_name* **[-noconfirm]**

Web Element Manager Path

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

integrity-algorithm-lte

Choose the order of preference for using an Integrity Algorithm.

CLI (Call Control Profile Configuration Mode)

integrity-algorithm-lte priority1 { 128-eia0 | 128-eia1 | 128-eia2 } priority2 128-eia { 0 | 1 | 2 } priority3 128-eia { 0 | 1 | 2 }

Web Element Manager Path

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

imei

Defines a range of IMEI (International Mobile Equipment Identity) numbers and associates an IMEI profile with the range definition.

CLI (Operator Policy Configuration Mode)

imei range *IMEI_number* **to** *IMEI_number* **{ imei-profile** *profile_name* **| sv** *##* **imei-profile** *profile_name* **}**

Web Element Manager Path

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

lac

Configures a 3G location area code or area codes where a UE, associated with this MME policy, is restricted from participating in a handover scenario.

CLI (MME Forbidden Location Area Configuration Mode)

[no] lac { *area_code* **} +**

Web Element Manager Path

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

lac

Configures a 3G location area code or area codes that define this pool area.

CLI (MME LAC Pool Area Configuration Mode)

[no] lac { *area_code* **} +**

Web Element Manager Path

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

mmemgr-recovery

Configures the recovery action for the MME manager.

CLI (MME Service Configuration Mode)

mmemgr-recovery { no-reset | reset }

Web Element Manager Path

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

mme-offload

Initiates or stops the offload of UEs associated with a specified MME service.

CLI (Exec Mode)

mme offload mme-service *name* **{ start mme-init-release-timeout** *seconds* **paginginit-timeout** *seconds* **| stop }**

Web Element Manager Path

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

mme-policy

This command enters the MME Policy Configuration Mode where MME policy parameters can be configured.

CLI (Global Configuration Mode)

mme-policy

Web Element Manager Path

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

mme-reset

Sends an S1 RESET message to a designated EnodeB to reset all UE-associated S1 connections.

CLI (Exec Mode)

mme reset s1-peer *peer_id*

Web Element Manager Path

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

max-bearers-per-subscriber

Define the maximum number of bearers allowed per subscriber.

CLI (Call Control Profile Configuration Mode)

max-bearers-per-subscriber *number*

Web Element Manager Path

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

max-pdns-per-subscriber

Define the maximum number of PDNs allowed per subscriber.

CLI (Call Control Profile Configuration Mode)

max-pdns-per-subscriber *number*

Web Element Manager Path

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

non-pool-area

Configures a non-pool area where a group of LAC values use a specific VLR.

CLI (MME SGs Service Configuration Mode)

non-pool-area *name* **use-vlr** *vlr_name* **lac** *value(s)*

Web Element Manager Path

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

operator-policy

This command creates an operator policy and enters the operator policy configuration mode.

CLI (Global Configuration Mode)

operator-policy (default | name *policy_name* **} [-noconfirm]**

Web Element Manager Path

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

peer-mme

Configures parameters that, when matched by another MME, specifies that MME as a peer for inter-MME relocations.

CLI (MME Service Configuration Mode)

peer-mme { gummei mcc *number* **mnc** *number* **group-id** *id* **mme-code** *code* **address** *ipv4_address* **| tai-match priority** *value* **mcc** *number* **mnc** *number* **tac {** *area_code* **| any |** *start_area_code* **to** *end_area_code* **} address** *ipv4_address* **}**

Web Element Manager Path

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

pgw-address

Configures the IPv4 or IPv6 address of the P-GW supporting the APN associated with this APN profile.

CLI (APN Profile Configuration Mode)

gateway-address *ip_address* **{ s5-s8-protocol pmip | weight** *weight* **}**

Web Element Manager Path

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

plmn-protocol

Configure the protocol supported by the PLMN.

CLI (Call Control Profile Configuration Mode)

plmn-protocol plmnid mcc *mcc_num* **mnc** *mnc_num* **[s5-protocol | s8-protocol] [gtp | pmip]**

Web Element Manager Path

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

policy network

This command configures the MME to indicate to the P-GW that all peer SGSNs support dual-addressing for bearers and, subsequently, dual-addressing must be supported for all IPv4 and IPv6 PDNs. Dual-addressing on SGSNs is based on UE capability to support inter-rat roaming.

CLI (MME Service Configuration Mode)

[default | no] policy network dual-addressing-supported

Web Element Manager Path

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

policy s1-reset

This command configures how the MME responds to an S1 interface reset.

CLI (MME Service Configuration Mode)

policy s1-reset { detach-ue | idle-mode-entry }

Web Element Manager Path

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

policy sctp-down

This command configures how the MME responds to a failure of the SCTP connection from the eNodeB.

CLI (MME Service Configuration Mode)

policy sctp-down { detach-ue | idle-mode-entry }

Web Element Manager Path

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

pool-area

Creates a LAC pool are configuration or specifies an existing pool area and enters the LAC Pool Area Configuration Mode.

CLI (MME SGs Service Configuration Mode)

[no] pool-area *pool_name* **[-noconfirm]**

Web Element Manager Path

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

precedence

Sets the order of precedence, the matching criteria and the association to an operator policy for subscribers meeting the match criteria.

CLI (MME Subscriber Map Configuration Mode)

precedence *number* **match-criteria all operator-policy-name** *policy_name*

precedence *number* **match-criteria imsi mcc** *mcc_num* **mnc** *mnc_num* **[msin first** *start_range* **last** *end_range* **| service-plmnid** *id* **] operator-policy-name** *policy_name*

precedence *number* **match-criteria service-plmnid** *id* **operator-policy-name** *policy_name*

Web Element Manager Path

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

qos

Configure quality of service parameters to be applied.

CLI (Call Control Profile Configuration Mode)

```
qos gn-gp { arp high-priority priority medium-priority priority |
pre-emption { capability { may-trigger-pre-emption |
shall-not-trigger-pre-emption } | vulnerability { not-pre-emptable |
pre-emptable }
```

Web Element Manager Path

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

qos apn-ambr

Configures the APN-AMBR (aggregate maximum bit rate) that will be stored in the HSS.

CLI (APN Profile Configuration Mode)

```
qos apn-ambr max-ul mbr-up max-dl mbr-dwn
```

Web Element Manager Path

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

qos dedicated-bearer

Configures the quality of service parameters for the dedicated bearer.

CLI (APN Profile Configuration Mode)

```
qos dedicated-bearer mbr max-ul mbr-up max-dl mbr-dwn
```

Web Element Manager Path

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

qos default-bearer

Configures the quality of service parameters for the default bearer. This command is specific to the MME.

CLI (APN Profile Configuration Mode)

```
qos default-bearer { arp arp_value [ preemption-capability { may |
shall-not } | vulnerability { not-preemptable | preemptable } ] | qci qci }
```

Web Element Manager Path

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

rfsp-override

Configure RAT frequency selection priority override parameters for this call-control profile.

CLI (Call Control Profile Configuration Mode)

```
rfsp-override { default | ue-val value new-val value }
```

Web Element Manager Path

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

s1-reset

Configure behavior of user equipment (UE) on S1-reset.

CLI (Call Control Profile Configuration Mode)

s1-reset { detach-ue | idle-mode-entry }

Web Element Manager Path

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

sctp

Configures the Stream Control Transmission Protocol (SCTP) port number for this service.

CLI (MME SGs Service Configuration Mode)

sctp port *port_number*

Web Element Manager Path

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

sctp-down

Configure behavior towards UE (user equipment) when SCTP goes down.

CLI (Call Control Profile Configuration Mode)

sctp-down { detach-ue | idle-mode-entry }

Web Element Manager Path

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

sgs-service

This command creates an SGS service instance and enters the SGS Service Configuration Mode.

CLI (Context Configuration Mode)

sgs-service *name* **[-noconfirm]**

Web Element Manager Path

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

sgw-address

Configures an S-GW IP address, supported S5/S8 protocol type, and selection weight used in a pool for S-GW selection.

CLI (MME TAI Management Object Configuration Mode)

sgw-address *ipv4_or_ipv6_address* **s5-s8-protocol { both | gtp | pmip } weight** *number*

Web Element Manager Path

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

subscriber-map

Creates a subscriber map or specifies an existing subscriber map and enters the Subscriber Map Configuration Mode.

CLI (MME Policy Configuration Mode)

[no] subscriber-map *map_name* **[-noconfirm]**

Web Element Manager Path

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

tac

Configures a tracking area code or area codes where a UE, associated with this MME policy, is restricted from participating in a handover scenario.

CLI (MME Forbidden Tracking Area Configuration Mode)

[no] tac *area_code*

Web Element Manager Path

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

tac-to-lac-mapping

Maps any TAC value or a specific TAC value to a LAC value.

CLI (MME SGs Service Configuration Mode)

tac-to-lac-mapping { any-tac | tac *value* **} map-to lac** *value*

Web Element Manager Path

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

tai

Configures a Tracking Area Identifier (TAI) for this TAI management object.

CLI (MME TAI Management Object Configuration Mode)

[no] tai mcc *number* **mnc** *number* **{ tac value } +**

Web Element Manager Path

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

tai-mgmt-db

Creates a Tracking Area Identifier (TAI) Management Database or specifies an existing database and enters the TAI Management Database Configuration Mode.

CLI (MME Policy Configuration Mode)

[no] tai-mgmt-db *db_name* **[-noconfirm]**

Web Element Manager Path

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

tai-mgmt-obj

Creates new, or removes/enters existing, MME Tracking Area Identifier (TAI) object configurations.

CLI (MME TAI Management Database Configuration Mode)

[no] tai-mgmt-obj *object_name* **[-noconfirm]**

Web Element Manager Path

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

tau

Configure parameters for tracking area update (TAU) procedure.

CLI (Call Control Profile Configuration Mode)

tau { imei-query-type { imei [verify-equipment-identity] | imei-sv [verify-equipment-identity] | none } | inter-rat { allow-mapped | native } }

Web Element Manager Path

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

treat-as-hplmn

Enable/disable the MME or SGSN to treat an IMSI series as coming from the home PLMN.

CLI (Call Control Profile Configuration Mode)

[remove] treat-as-hplmn

Web Element Manager Path

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

vlr

Configures the Visitor Location Register (VLR) to be used by this service.

CLI (MME SGs Service Configuration Mode)

vlr *vlr_name* **ipv4-address** *ip_address* **port** *port_number*

Web Element Manager Path

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

wildcard-apn

Enable/disable the Wildcard APN feature and define the APN to be used in case a wildcard APN is included in the subscriber record.

CLI (APN Remap Table Configuration Mode)

wildcard-apn pdp-type { ipv4 | ipv6 | ppp } apn-network-identifier *apn_net_id*

Web Element Manager Path

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

NAT Commands - New in Release 11.0

This section provides information on new NAT commands available in Release 11.0.

flow check-point

This command checkpoints all the flows matching the Firewall-and NAT action.

CLI (Firewall-and-NAT Action Configuration Mode)

flow check-point [data-usage *data_usage* **[and | or] | time-duration** *duration* **[and | or]]**

Web Element Manager Path

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

Packet Data Network Gateway Commands - New in Release 11.0

This section provides information on new Packet Data Network Gateway (P-GW) commands available in Release 11.0.

event-report-indication

This command enables event report indication.

CLI (Exec Mode)

event-report-indication { all | pgw-trace-control | qos-change | rai-change | rat-change | sgsn-change | ue-timezone-change | user-loc-change } [pgw-trace-control] [qos-change] [rai-change] [rat-change] [sgsn-change] [ue-timezone-change] [user-loc-change]

{ default | no } event-report-indication

Web Element Manager Path

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

event-update

This command enables event report indication.

CLI (Exec Mode)

event-update send-usage-report [reset-usage]

{ default | no } event-update

Web Element Manager Path

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

ipsec-allow-error-ind-in-clear

This command configures whether error-indication is dropped or sent without IPSec tunnel.

CLI (Exec Mode)

[default | no] ipsec-allow-error-ind-in-clear

Web Element Manager Path

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

ipsec-tunnel-idle-timeout

This command configures the IPSec tunnel idle timeout after which IPSec tunnel deletion is triggered.

CLI (Exec Mode)

ipsec-tunnel-idle-timeout *seconds*

default ipsec-tunnel-idle-timeout

Web Element Manager Path

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

PDIF Commands - New in Release 11.0

None for this release.

PDSN Commands - New in Release 11.0

None for this release.

Peer-to-Peer - New in Release 11.0

None for this release.

Serving Gateway Commands - New in Release 11.0

This section provides information about new Serving Gateway (S-GW) commands.

ca-crl

Configures the name and URL path of a Certificate Authority-Certificate Revocation List (CA-CRL).

CLI (Global Configuration Mode)

ca-crl name *name* **{ der | pem } { url** *url* **}**

Web Element Manager Path

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

ca-crl list

Binds one or more Certificate Authority-Certificate Revocation Lists (CA-CRLs) to this crypto template.

CLI (Crypto Template Configuration Mode)

ca-crl list ca-crl-name *name* **[ca-crl-name** *name* **] +**

Web Element Manager Path

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

peer network

Configures a list of allowed peer addresses on this crypto template.

CLI (Crypto Template Configuration Mode)

peer network *ip_address* **{***/mask* **| mask** *ip_mask* **} [encrypted pre-shared-key** *key* **| pre-shared-key** *key* **]**

Web Element Manager Path

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

plmn

Configures the PLMN identifier for this S-GW service.

CLI (S-GW Service Configuration Mode)

plmn id mcc *number* **mnc** *number* **[primary]**

Web Element Manager Path

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

Session Control Manager Commands - New in Release 11.0

This section provides information on new commands available in Release 11.0.

3gpp

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

CLI (CSCF Serving-CSCF Configuration Mode)

3gpp Rel8 Cx { alias-indication | dynamic-password-change | ims-restoration | num-auth-vectors *value* **}**

[default | no] 3gpp Rel8 Cx { alias-indication | dynamic-password-change | ims-restoration | num-auth-vectors }

Web Element Manager Path

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

after

Places the subdomain-route at the bottom or end of the subdomain-routes list. Use this command in conjunction with the **route** command.

CLI (CSCF Subdomain-route List Configuration Mode)

after

Web Element Manager Path

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

authorization

Enables P-CSCF to authorize calls for all supported media types; both video and non-video calls will be authorized using external PCRF via Rx. Default is enabled.

CLI (CSCF Proxy-CSCF Configuration Mode)

[no] authorization non-video

Web Element Manager Path

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

before

Places the subdomain-route at the bottom or end of the subdomain-routes list. Use this command in conjunction with the **route** command.

CLI (CSCF Subdomain-route List Configuration Mode)

before

Web Element Manager Path

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

cscf subdomain-routes

Creates/removes a subdomain-route list and/or enters the Subdomain-route List Configuration Mode.

CLI (Context Configuration Mode)

`[ no ] cscf subdomain-routes`

Web Element Manager Path

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

monitoring

Enables thresholds alerting for a CSCF service.

CLI (CSCF Service Configuration Mode)

`monitoring`

Web Element Manager Path

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

route

Creates a route entry to be used in the subdomain-routes list for the I-CSCF.

CLI (CSCF Subdomain-route List Configuration Mode)

`[ no ] route peer-servers` *`name`* **`[ log ] base-criteria destination aor`** *`aor`*

Web Element Manager Path

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

subscribe

Enables subscription to signalling bearer loss via PCRF.

CLI (CSCF Proxy-CSCF Configuration Mode)

`[ no ] subscribe signaling-bearer-loss`

Web Element Manager Path

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

support-content-type

Validates Content-Type in a CSCF service.

CLI (CSCF Service Configuration Mode)

`[ no ] support-content-type any`

Web Element Manager Path

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

SGSN Commands - New in Release 11.0

This section provides information on new commands available in Release 11.0.

access-restriction-data

A new command enables the operator to assign a failure code to be included in reject messages if attach rejection is due to access restriction data (ARD) checking of incoming subscriber data (ISD) messages. As well, the operator can disable the ARD checking behavior.

CLI (Call-Control Profile Configuration Mode)

access-restriction-data { failure-code *<cause_code>* **| no-check }**

apn-profile

A new command creates one of the key elements of the new optimized Operator Policy feature - an APN profile instance and enters the APN Profile configuration mode.

CLI (Global Configuration Mode)

apn-profile *profile_name*

no apn-profile *profile_name*

apn-remap

This command creates an entry in the APN remap table to define various APN overrides. This command requires the APN Aliasing license.

CLI (APN Remap Table Configuration Mode)

apn-remap { network-identifier *apn_net_id* **{ new-ni** *new_apn_net_id* **| operator-identifier** *apn_op_id* **new-ni** *new_apn_net_id* **{ new-oi** *new_apn_op_id* **| value-for-oi-mcc** *mcc* **| value-for-oi-mnc** *mnc* **} | value-for-ni-wc** *new_apn_net_id* **} | operator-identifier** *apn_op_id* **{ new-oi** *new_apn_op_id* **| value-for-oi-mcc** *mcc* **| value-for-oi-mnc** *mnc* **} }**

no apn-remap { network-identifier *apn_net_id* **| operator-identifier** *apn_op_id* **}**

apn-remap-table

A new command creates one of the key elements of the optimized Operator Policy feature and the APN Aliasing feature - an APN remap table instance and enters the APN Remap Table configuration mode.

CLI (Global Configuration Mode)

apn-remap-table *table_name*

no apn-remap-table *table_name*

associate-sccp-network

This command associates an instance of an SCCP network configuration with a CAMEL service instance.

CLI (CAMEL Service Configuration Mode)

associate-sccp-network *sccp_network_id*

no associate-sccp-network

blank-apn

This command enables the Blank APN feature which is part of the APN Aliasing features set and requires the APN Aliasing license.

CLI (APN Remap Table Configuration Mode)

blank-apn network-identifier *<apn_net_id>*

no blank-apn

bssgp-timer

New command configures the T2 and TH timers for the BVCs (BSSGP virtual connections) of the NSE (network service entities).

CLI (SGSN-Global Configuration Mode)

bssgp-timer { t2 *T2_time* **| th** *TH_time* **}**

default bssgp-timer { t2 | th }

call-control-profile

A new command creates one of the key elements of the new optimized Operator Policy feature - an call-control profile instance and enters the Call-Control Profile configuration mode.

CLI (Global Configuration Mode)

call-control-profile *profile_name*

no call-control-profile *profile_name*

camel-service

This command creates an instance of a CAMEL service and enters the CAMEL Service Configuration Mode.

CLI (Context Configuration Mode)

camel-service *service_name*

no camel-service *service_name*

direct-tunnel-disabled-ggsn

New command allows the operator to disable direct tunnel on the basis of an GGSN IP address.

CLI (SGTP Service Configuration Mode)

direct-tunnel-disabled-ggsn *<IPv4/IPv6_address>*

no direct-tunnel-disabled-ggsn [*IPv4/IPv6_address* **]**

dns-extn

New command takes an offset group of digits from the MSISDN and appends the digits to the DNS query string to create a new APN to assist roaming subscribers to use the local GGSN.

CLI (APN Profile Configuration Mode)

dns-extn msisdn start-offset <*start_digit*> end-offset <*end_digit*>

imei-profile

A new command creates one of the key elements of the new optimized Operator Policy feature - an IMEI profile instance and enters the IMEI Profile configuration mode.

CLI (Global Configuration Mode)

imei-profile *profile_name*

no imei-profile *profile_name*

imsi-range

A new command configure an IMSI range or a PLMN ID to associate with an Operator Policy.

CLI (SGSN-Global Configuration Mode)

imsi-range mcc *mcc_num* **mnc** *mnc_num* **{ msin first** *start_number* **last** *stop_number* **operator-policy** *policy_name* **| plmnid** *plmn_id* **operator-policy** *policy_name* **} +**

no imsi-range mcc *mcc_num* **mnc** *mnc_num* **{ msin first** *start_number* **last** *stop_number* **| plmnid** *plmn_id* **}**

link

Multiple new commands have been added to the Link configuration mode to set timers for the newly enabled narrowband SS7 MTP2 layer:

CLI (Link Configuration Mode)

[default] mtp2-aerm-emergency-threshold <*1..50***>**

[default] mtp2-aerm-normal-threshold <*4..100***>**

[default] mtp2-eim-decrement <*1..2***>**

[default] mtp2-eim-increment <*1..2***>**

[default] mtp2-eim-threshold <*100..200***>**

[default] mtp2-error-correction {*basic | preventive-cyclic-retransmission***}**

[default] mtp2-lssu-len <*1..2***>**

[default] mtp2-suerm-threshold <*64..1023***>**

[default | no] timeout mtp2-tmr-t1 <*250..3500 | 400..500***>**

[default | no] timeout mtp2-tmr-t2 <*50..150***>**

[default | no] timeout mtp2-tmr-t3 <*10..20***>**

[default] timeout mtp2-tmr-t4e <*4..6***>**

[default] timeout mtp2-tmr-t4n <*30..700 | 75..95***>**

[default | no] timeout mtp2-tmr-t5 <*1..2***>**

[default | no] timeout mtp2-tmr-t6 <*30..60***>**

[default | no] timeout mtp2-tmr-t7 <*5..20*>

[default | no] timeout mtp2-tmr-t8 <*1..2*> (high speed only)

link-type

In the Linkset configuration mode, to enable SS7 narrowband, the user must use the **link-type** keyword (with the **link** command) to select either high-speed-narrowband (HS) or low-speed-narrowband (LS). The commands have been visible in earlier releases but only enabled in this release:

CLI (Linkset Configuration Mode)

link id <*1-16*> link-type { atm-broadband | highspeed-narrowband | lowspeed-narrowband }

max-pending-attaches

A new command allows the operator to set a limit to the pending queues for Attach and RAU messages (default 10000 entries).

CLI (SGSN-Global Configuration Mode)

max-pending-attaches *limit*

default max-pending-attaches

operator-policy

A new command creates one of the key elements of the new optimized Operator Policy feature - an operator policy and enters the Operator Policy configuration mode.

CLI (Global Configuration Mode)

operator-policy { default | name *policy_name* **}**

no operator-policy { default | name *policy_name* **}**

sgtpc test echo sgsn-address

This command initiates a test for the GTPC echo procedure -- echo from the specified SGSN to a specified GGSN or to all GGSNs that have sessions with the SGTP service. This command should be issued from the context in which the SGTP service is configured.

CLI (Exec Mode)

sgtpc test echo sgsn-address <*SGSN_IP_address*> {all | ggsn-address <*GGSN_IP_address*> }

timeout

This command defines the various timers required for the CAMEL service.

CLI (CAMEL Service Configuration Mode)

timeout { gprs-apply-charging-report-ack-timer *seconds* **| gprs-entity-release-ack-timer** *seconds* **| gprs-event-report-ack-timer** *seconds* **| gprs-tssf-timer** *seconds* **| sms-event-report-ack-timer** *seconds* **| sms-tssf-timer** *seconds* **| tc-guard-timer** *seconds* **}**

default timeout { gprs-apply-charging-report-ack-timer | gprs-entity-release-ack-timer | gprs-event-report-ack-timer | gprs-tssf-timer | sms-event-report-ack-timer | sms-tssf-timer | tc-guard-timer }

umts-aka-r99

New command allows the operator to authenticate MEs, with R99+ USIMs and capable of UMTS AKA, that are attempting to connect to a 2G network.

CLI (SGSN-Global Configuration Mode)

umts-aka-r99

no umts-aka-r99

Modified Configuration Commands

This section contains configuration commands that have been modified in Release 11.0. Modified commands in this version are divided into the following sections:

Common Commands - Modified in Release 11.0

This section provides information on common commands modified in Release 11.0.

event-update

This command sends volume usage information when the event change is reported to PCRF in CCR-U message. A new keyword **reset-usage** is added to support delta reporting wherein the usage is reported and reset at PCEF.

CLI (Credit Control Configuration Mode)

event-update send-usage-report [reset-usage]

Web Element Manager Path

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

gtpp group

This command enables a configured GTPP server group to an APN for CGF accounting functionality. In this release, this command can be used to configure up to a maximum of 32 groups for each APNs.

CLI (APN Configuration Mode)

gtpp group *group_name* **[accounting-context** *ac_context_name* **]**

[no | default] gtpp group *group_name*

Web Element Manager Path

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

ip qos-dscp

This command configures the quality of service (QoS) differentiated service code point (DSCP) used when sending data packets over the Gn interface.

CLI (GGSN Service Configuration Mode and APN Configuration Mode)

ip qos-dscp { qci { 1 { dscp } | 2 { dscp } | 3 { dscp } | 4 { dscp } | 5 { dscp | allocation-retention-priority } | 6 { dscp | allocation-retention-priority } | 7 { dscp | allocation-retention-priority } | 8 { dscp | allocation-retention-priority } | 9 { dscp }} | gtpc } +

[no] ip qos-dscp { qci { 1 | 2 | 3 | 4 | 5 { allocation-retention-priority | dscp } | 6 { allocation-retention-priority | dscp } | 7 { allocation-retention-priority | dscp } | 8 { allocation-retention-priority | dscp } | 9 } | gtpc } +

Web Element Manager Path

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

qos-class-identifier

This command configures the QoS Class Identifier. This command now supports configuring QCI values between 1–9 and 128–254.

CLI (ACS Charging Action Configuration Mode)

qos-class-identifier *identifier*

no qos-class-identifier

Web Element Manager Path

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

qos negotiate-limit

This command configures the QoS profile to provide the peak and committed data rate limits that the GGSN assigns to the APN, and sends to the SGSNs in response to GTP create/update PDP context requests for traffic shaping and policing functionality.

CLI (APN Configuration Mode)

qos negotiate-limit direction { downlink | uplink } [qci *qci_val* **] [peak-data-rate** *bps* **[committed-data-rate** *bps* **] | committed-data-rate [peak-data-rate** *bps* **]]**

no qos negotiate-limit direction { downlink | uplink } [class { background | conversational | interactive *traffic_priority* **| streaming }]**

Web Element Manager Path

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

qos rate-limit

This command configures the action on subscriber traffic flow that violates or exceeds the peak/committed data rate under traffic policing/shaping functionality.

CLI (APN Configuration Mode)

qos rate-limit { downlink | uplink } [qci *qci_val* **] [burst-size { bytes | auto-readjust [duration** *dur* **] }] [exceed-action { drop | lower-ip-precedence | transmit } [violate-action { drop | lower-ip-precedence | shape [transmit-when-buffer-full] | transmit }]] | [violate-action { drop | lower-ip-precedence | shape [transmit-when-buffer-full] | transmit } [exceed-action { drop | lower-ip-precedence | transmit }]] +**

no qos rate-limit direction { downlink | uplink } [qci *qci_val* **]**

Web Element Manager Path

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

sgsn-failures

A new logging facility- **sgsn-failures** – has been added to configure and enable logging of SGSN call attempt failures.

CLI (Exec Mode)

logging filter active facility sgsn-failures level *<level_type>*

sgsn-failures

A new logging facility- **sgsn-failures** – has been added to configure and enable logging of SGSN call attempt failures:

CLI (Global Configuration Mode)

logging filter runtime facility sgsn-failures level *<level_type>*

sgsn-failures

CLI (Exec Mode)

A new logging facility- sgsn-failures – has been added to configure and enable logging of SGSN call attempt failures:

CLI (Exec Mode)

show logs [active | inactive | callid *call_id* **| event-verbosity** *evt_verboseness* **] [facility sgsn-failures]**

trigger type

This command enables or disables triggering a credit reauthorization when the named values in the subscriber session changes.

The keyword **serving-node** is now available with this command. This keyword indicates that a change in serving node shall cause the credit control client to ask for a re-authorization of the associated quota.

CLI (Credit Control Configuration Mode)

[no] trigger type { cellid | lac | qos | rat | serving-node | sgsn } +

Web Element Manager Path

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

usage-reporting

This command configures the ACS Credit Control usage reporting type. A new optional keyword **report-only-granted-volume** is available with this command.

When this keyword is not configured the CLI will not send CC-TIME and CC-SERVICE-UNITS or whatever units that is not present in the GSU. If the GSU comes with CC-Total-Octets, the total, input and output octets is sent in USU. This keyword will enable input and output octets to be suppressed. With the keyword the CLI will strictly follow what is present in the GSU. If it comes with Total-Octets, only Total-Octets is sent in USU.

CLI (Credit Control Configuration Mode)

usage-reporting quotas-to-report based-on-grant [report-only-granted-volume]

default usage-reporting quotas-to-report

Web Element Manager Path

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

Content Filtering Commands - Modified in Release 11.0

None for this release.

ECS Commands - Modified in Release 11.0

This section provides information on ECS commands modified in Release 11.0.

charging-rule-optimization

This command specifies the internal optimization level to use when evaluating instances of the **`action`** CLI command. The following changes were made to this command:

- The rule-optimization level medium has been deprecated.
- The default rule-optimization level has been changed to high.

CLI (ACS Rulebase Configuration Mode)

```
charging-rule-optimization { high | low }
default charging-rule-optimization
```

Web Element Manager Path

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

Firewall Commands - Modified in Release 11.0

None for this release.

GGSN Commands - Modified in Release 11.0

This section provides information on GGSN commands modified in Release 11.0.

gtpp dictionary

Ten new options: custom31... custom40, have been added to the **`dictionary.`** These are custom defined dictionaries for SGSN only.

CLI (GTPP Server Group Configuration Mode)

```
gtpp dictionary { custom1 | custom10 | custom11 | custom12 | custom13 |
custom14 | custom15 | custom16 | custom17 | custom18 | custom19 | custom20
| custom21 | custom22 | custom23 | custom24 | custom25 | custom26 |
custom27 | custom28 | custom29 | custom3 | custom30 | custom31 | custom32 |
custom33 | custom34 | custom35 | custom36| custom37 | custom38 | custom39 |
custom4 | custom40 | custom5 | custom6 | custom7 | custom8 | custom9 |
standard }
```

Web Element Manager Path

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

gtpp storage-server local file

Two new options: custom7 and custom 8, have been added to the **format** keyword to allow the use of custom 7 and custom 8 CDR file formats.

Also, the default value of volume option decreased from 10MB to 4MB.

CLI (Context Configuration Mode)

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

Web Element Manager Path

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

name format

A new keyword has been added to allow the format of CDR filenames to be configured independently from the file format. The format string includes % as a format specifier to add % to the file name.

CLI (GTPP Server Group Configuration Mode)

[no] gtpp storage-server local file name format *string_1-127* **[max-file-seq-no** *<1- 4294967295>* **]**

Web Element Manager Path

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

name prefix

A new value, null, has been added to the **prefix** keyword to allow the use of ‘no prefix’.

CLI (GTPP Server Group Configuration Mode)

gtpp storage-server local file name prefix

Web Element Manager Path

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

session trace

The **session trace** command modified to support GGSN as network entity to provide subscriber-level session trace support in Global configuration mode.

CLI (Global Configuration Mode)

session trace [collection-timer *sec* **] [network-element { all | ggsn | mme | pgw | sgw }] [retry-timer** *sec* **] [tce-mode { none | push transport { ftp | sftp } path** *string* **username** *name* **{ encrypted password** *enc_pw* **| password** *password* **} }]**

no session trace [network-element { all | ggsn | mme | pgw | sgw }]

Web Element Manager Path

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

session trace subscriber

The **session trace subscriber** command modified to support GGSN as network entity to provide subscriber-level session trace support in Exec mode. It also now supports Gi, Gmb, Gn, and Gx interface for session trace collection.

CLI (Exec Mode)

session trace subscriber network-element { ggsn | mme | pgw | sgw } { imei *id* **} { imsi** *id* **} { interface { all | interface } } trace-ref** *id* **collection-entity** *ip_address*

no session trace subscriber [network-element { ggsn | mme | pgw | sgw }] [trace-ref *id* **]**

Web Element Manager Path

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

virtual-apn

Virtual APN command modified to support generalized virtual APN usage and has been extended for the other (non-UMTS) products as well.

CLI (APN Configuration Mode)

virtual-apn { gcdr apn-name-to-be-included { gn | virtual } | preference *priority* **apn** *apn_name* **{ domain** *domain_name* **| mcc** *mcc_number* **mnc** *mnc_number* **bearer-access-service-name** *svc-name* **| access-gw-address {** *ip_address* **|** *ip_address/mask* **} | roaming-mode { home | visiting | roaming } } }**

Web Element Manager Path

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

HA Commands - Modified in Release 11.0

None for this release.

Mobility Management Entity Commands - Modified in Release 11.0

This section provides information on Mobility Management Entity (MME) commands modified in Release 11.0.

associates

The following keywords have been removed from this command:

mme-hhs-service *hss_svc_name*

The following keywords have been added to this command:

hss-peer-service *hss_svc_name* **| sgsservice** *sgs_svc_name* **| sgtpc-service** *sgtpc_svc_name*

CLI (MME Service Configuration Mode)

associate { { egtp-service *egtp_svc_name* **| hss-peer-service** *hss_svc_name* **| sgs-service** *sgs_svc_name* **| sgtpc-service** *sgtpc_svc_name* **} [context** *ctx_name* **] | subscriber-map** *map_name* **| tai-mgmt-db** *database_name* **}**

Web Element Manager Path

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

bind s1-mme

The following keywords have been removed from this command:

address *address*

The following keywords have been added to this command:

{ ipv4-address *address* **[ipv4-address** *secondary_address* **] | ipv6-address** *address* **[ipv6-address** *secondary_address* **]**

CLI (MME Service Configuration Mode)

bind s1-mme { ipv4-address *address* **[ipv4-address** *secondary_address* **] | ipv6-address** *address* **[ipv6-address** *secondary_address* **] } [max-subscribers** *number* **]**

Web Element Manager Path

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

failure-handling

This command configures the failure handling behavior in the event of a failure with the HSS peer service. It also defines the action on various error codes on Diameter interface during authentication or session activities.

IMPORTANT

This command was previously in the MME-HSS Service Configuration Mode which has been obsoleted in release 11.0.

CLI (HSS Peer Service Configuration Mode)

failure-handling { authentication-information-request | check-identity-request | notify-request | purge-ue-request | update-location-request } { diameter-result-code *start_error_code* **[to** *end_error_code* **] | request-timeout } action { continue | retry-and-terminate | terminate }**

Web Element Manager Path

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

policy attach

The following keywords have been removed from this command:

eir-query { enable | disable }

The following keywords have been added to this command:

imei-query-type { imei | imei-sv | none } [verify-equipmentidentity [deny-greylisted]]

CLI (MME Service Configuration Mode)

policy attach { imei-query-type { imei | imei-sv | none } [verify-equipmentidentity [deny-greylisted]] | set-ue-time { disable | enable }

Web Element Manager Path

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

policy tau

The following keywords have been removed from this command:

```
eir-query { enable | disable }
```

The following keywords have been added to this command:

```
imei-query-type { imei | imei-sv | none } [ verify-equipmentidentity [
deny-greylisted ] ]
```

CLI (MME Service Configuration Mode)

```
policy tau { imei-query-type { imei | imei-sv | none }
[ verify-equipmentidentity [ deny-greylisted ] ] | set-ue-time { disable |
enable }
```

Web Element Manager Path

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

request timeout

This command configures the application request timeout between HSS peer service and HSS node. The MME system will wait for this duration before retransmitting the request to corresponding HSS node.

IMPORTANT

This command was previously in the MME-HSS Service Configuration Mode which has been obsoleted in release 11.0.

CLI (HSS Peer Service Configuration Mode)

request timeout *dur*

Web Element Manager Path

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

NAT Commands - Modified in Release 11.0

This section provides information on NAT commands modified in Release 11.0.

access-rule

This command creates and configures an access rule. This command now supports the check-pointing of NATed flows.

CLI (Firewall-and-NAT Policy Configuration Mode)

access-rule { no-ruledef-matches { downlink | uplink } action { deny [charging-action *charging_action* **] | permit [bypass-nat | nat-realm** *nat_realm* **[fw-and-nat-action** *name* **]] } | priority** *priority* **{ [dynamic-only | static-and-dynamic] access-ruledef** *ruledef_name* **{ deny [charging-action** *charging_action* **] | permit [[bypass-nat | nat-realm** *nat_realm* **[fw-and-nat-action** *name* **]] trigger open-port {** *port_number* **| range** *start_port* **to** *end_port* **} direction { both | reverse | same }] } } }**

Web Element Manager Path

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

flow idle-timeout

This command configures the maximum duration a flow can remain idle after which the system automatically terminates the flow. This command now supports the Flow Mapping Timer to hold the resources (NAT IP, NAT port, Private IP NPU flow) associated with a 5-tuple flow until Mapping timeout expiry.

CLI (ACS Charging Action Configuration Mode)

flow idle-timeout { *idle_timeout* **| flow-mapping** *flow_timeout* **}**

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. This command now supports the Flow Mapping Timer to hold the resources (NAT IP, NAT port, Private IP NPU flow) associated with a 5-tuple flow until Mapping timeout expiry.

CLI (ACS Configuration Mode)

idle-timeout { alg-media | flow-mapping { tcp | udp } | icmp | tcp | udp } *idle_timeout*

Web Element Manager Path

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

Packet Data Network Gateway Commands - Modified in Release 11.0

This section provides information on Packet Data Network Gateway (P-GW) commands modified in Release 11.0.

accounting-event-trigger

This command configures the response to specific event triggers for a policy. The following keywords were added:

- **cgi-sai-change** - Specifies that the action is initiated upon indication of a cgi-sai change.
- **ecgi-change** - Specifies that the action is initiated upon indication of an ecgi change.
- **rai-change** - Specifies that the action is initiated upon indication of an rai change.
- **tai-change** - Specifies that the action is initiated upon indication of a tai change.

CLI (Accounting Policy Service Configuration Mode)

```
accounting-event-trigger { cgi-sai-change | ecgi-change |
flow-information-change | interim-timeout | location-change | rai-change |
tai-change } action { interim | stop-start }
```

```
[ default | no ] accounting-event-trigger { cgi-sai-change | ecgi-change |
flow-information-change | interim-timeout | location-change | rai-change |
tai-change }
```

Web Element Manager Path

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

associate

The P-GW service can now be associated with an existing GGSN service within this context with the new keyword **ggsn-service** *name*.

CLI (P-GW Service Configuration Mode)

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

```
no associate { egtp-service | lma-service | qci-qos-mapping }
```

Web Element Manager Path

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

bind

This command Configures the IP address to use for GTP-U data packets. The following keywords were added:

- **crypto-template** *crypto_template* - Configures crypto template for IPSec, which enables IPSec tunneling for this GTP-U address. Must be followed by the name of an existing crypto template.
  crypto_template must be from 1 to 127 alpha and/or numeric characters.
- **ike-bind-address** *ip_address* - Configures an IKE bind address. Must be followed by IPV4 or IPv6 address; IP address type must be the same as the GTP-U address type.
  ipv4_address must be entered as a standard IPv4 address in dotted decimal notation.
  ipv6_address must be entered as a standard IPv6 address in colon-separated notation.

In addition, a GTP-U service can now support a maximum of 12 GTP-U endpoints/interfaces.

CLI (GTP-U Service Configuration Mode)

[no] bind { ipv4-address *ipv4_address* **[crypto-template** *crypto_template* **] [ike-bind-address {** *ipv4_address* **}] [ipv6-address** *ipv6_address* **] | ipv6-address** *ipv6_address* **[crypto-template** *crypto_template* **] [ike-bind-address {** *ipv6_address* **}] [ipv4-address** *ipv4_address* **] }**

Web Element Manager Path

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

bind address

Added ability to specify optional IPv4 HA/P-GW address to support DSMIP6 session using IPv4 transport. *ipv4_address* must be entered as a standard IPv4 address in dotted decimal notation.

CLI (LMA Service Configuration Mode)

bind address *ipv6_address* **[ipv4-address** *ipv4_address* **] [max-subscribers** *num* **]**

no bind address

Web Element Manager Path

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

cc

This command configures a charging characteristics profile, within the accounting profile configuration, for CDR generation. The new keyword **serving-nodes** *num* specifies the number of serving node changes (inter-serving node switchovers) after which the interim CDR is generated. In P-GW and S-GW, a partial record needs to be generated whenever there is a serving node address list overflow. Serving node is added to the CDR list during handover scenarios. *num* must be an integer value from 1 to 4. If an accounting policy is not configured, this value is 4.

CLI (Accounting Policy Service Configuration Mode)

cc profile *index* **{ buckets** *num* **| interval** *seconds* **| serving-nodes** num **| tariff time1** *min hrs* **[time2** *min hrs*...**time4** *min hrs* **] | volume { downlink** *octets* **{ uplink** *octets* **} | total** *octets* **| uplink** *octets* **{ downlink** *octets* **} } }**

default cc profile *index*

no cc profile *index* **{ buckets | interval | serving-nodes | tariff | volume }**

Web Element Manager Path

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

ip address alloc-method

This command configures the method by which an APN will obtain IP addresses for PDP contexts. The new keyword **allow-deferred** enables support for P-GW deferred address allocation. Default is disabled.

CLI (APN Configuration Mode)

ip address allocation-method { dhcp-proxy [allow-deferred] [prefer-dhcp-options] | dhcp-relay | local [allow-deferred] | no-dynamic [allow-deferred] } [allow-user-specified]

Web Element Manager Path

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

PDIF Commands - Modified in Release 11.0

None for this release.

PDSN Commands - Modified in Release 11.0

None for this release.

Peer-to-Peer - Modified in Release 11.0

This section provides information on Peer-to-Peer commands modified in Release 11.0.

p2p-detection protocol

This command configures the system to detect peer-to-peer (P2P) protocols. The following keywords were added to this command:

- armagetron
- blackberry
- citrix
- clubpenguin
- crossfire
- dofus
- facebook
- fiesta
- florensia
- funshion
- guildwars
- icecast
- isakmp
- kontiki
- maplestory
- meebo
- mgcp
- octoshape
- off
- ps3
- rmstream
- rfactor
- shoutcast
- splashfighter
- ssdp
- stealthnet
- stun
- teamspeak
- thunder
- tor
- truphone
- veohtv
- wii

- wmstream
- wofkungfu
- xdcc
- yourfreedom

CLI (ACS Rulebase Configuration Mode)

```
[ no ] p2p-detection protocol [ actsync | aimini | all | applejuice | ares
| armagettron | battlefd | bittorrent | blackberry | citrix | clubpenguin |
crossfire | ddlink | directconnect | dofus | edonkey | facebook | fasttrack
| feidian | fiesta | filetopia | florensia | freenet | fring | funshion |
gadugadu | gnutella | gtalk | guildwars | halflife2 | hamachivpn | iax |
icecast | imesh | iptv | irc | isakmp | iskoot | jabber | kontiki | manolito
| maplestory | meebo | mgcp | msn | mute | nimbuzz | octoshape | off | oovoo
| openft | orb | oscar | paltalk | pando | pandora | popo | pplive |
ppstream | ps3 | qq | qqgame | qqlive | quake | rdp | rfactor | rmstream |
secondlife | shoutcast | skinny | skype | slingbox | sopcast | soulseek |
splashfighter | ssdp | stealthnet | steam | stun | teamspeak | thunder | tor
| truphone | tvants | tvuplayer | uusee | veohtv | vpnx | vtun | warcft3 |
wii | winmx | winny | wmstream | wofkungfu | wofwarcraft | xbox | xdcc |
yahoo | yourfreetunnel | zattoo + ]
```

Web Element Manager Path

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

p2p protocol

This command configures the system to detect specific P2P protocols for charging purposes. This release now supports the following protocols:

- Armagettron
- Blackberry
- Citrix
- Clubpenguin
- Crossfire
- Dofus
- Facebook
- Fiesta
- Florensia
- Funshion
- Guildwars
- Icecast
- ISAKMP
- Kontiki
- Maplestory
- Meebo

- MGCP
- Octoshape
- OFF
- PS3
- Real Media Stream
- Rfactor
- Shoutcast
- Splashfighter
- SSDP
- StealthNet
- STUN
- TeamSpeak
- Thunder
- Tor
- Truphone
- Veoh TV
- WII
- Windows Media Stream
- World of Kungfu
- XDCC
- YourFreedom

CLI (ACS Ruledef Configuration Mode)

`[ no ] p2p protocol` *operator protocol*

Web Element Manager Path

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

Serving Gateway Commands - Modified in Release 11.0

This section provides information about modified Serving Gateway (S-GW) commands.

crypto template

The following keyword has been removed from this command:

`ikev2-pdif`

The following keyword has been added to this command:

`ikev2-dynamic`

CLI (MME Service Configuration Mode)

`crypto template` *`name`* **`ikev2-dynamic`**

Web Element Manager Path

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

Session Control Manager Commands - Modified in Release 11.0

The following commands have been modified in Release 11.0.

access-type

This command specifies the access types for IMS core.The following types have been added:

- 3gpp-e-utran-fdd: 3GPP Access Type
- 3gpp-e-utran-tdd: 3GPP Access Type
- ieee-80211n: WLAN Access Type
- ieee-8023: Ethernet Access Type
- ieee-8023a: Ethernet Access Type
- ieee-8023ab: Ethernet Access Type
- ieee-8023ae: Ethernet Access Type
- ieee-8023ak: Ethernet Access Type
- ieee-8023an: Ethernet Access Type
- ieee-8023aq: Ethernet Access Type
- ieee-8023e: Ethernet Access Type
- ieee-8023i: Ethernet Access Type
- ieee-8023j: Ethernet Access Type
- ieee-8023u: Ethernet Access Type
- ieee-8023y: Ethernet Access Type
- ieee-8023z: Ethernet Access Type

CLI (CSCF Service Configuration Mode)

access-type { type } access-profile { default | name *access_profile_name* **} | ue-ip-address-range name** *ue_ip_name* **{ address** *ip_address_mask* **| range** *start_ip_address end_ip_address* **}**

no access-type { type } [access-profile | ue-ip-address-range [name *ue_ip_name* **]]**

Web Element Manager Path

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

charging

This command enables Rf charging in this CSCF service for SIP messages. The default value is now Disabled.

CLI (CSCF Service Configuration Mode)

[default | no] charging

Web Element Manager Path

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

cscf ifc-filter-criteria

cscf ifc-spt-condition

cscf ifc-spt-group

cscf ifc-trigger-point

cscf isc-template

spt-condition

spt-group

filter-criteria

All ifc-filter-criteria, ifc-spt-condition, ifc-spt-group, ifc-trigger-point, and isc-template **name** changed to **id**.

id value changed from string to an integer from 1 through 200.

CLI (Context Configuration Mode)

cscf ifc-filter-criteria id *fc_id* **priority** *pri* **profile-part-indicator { registered | unregistered } app-server uri scheme { sip | sips }** *as* **as-default-handling { session-continue | session-terminate } [-noconfirm]**

| [service-info *info* **] [trigger-point** *tp_name* **] [-noconfirm] | [trigger-point** *tp_id* **] [-noconfirm]**

no cscf ifc-filter-criteria id *fc_id*

cscf ifc-spt-condition id cond_id **{ 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 id *cond_id*

cscf ifc-spt-group id *group_id* **[[-noconfirm] | reg-type { de-registration | initial-registration | re-registration } [-noconfirm]]**

no cscf ifc-spt-group id *group_id*

cscf ifc-trigger-point id *tp_id* **condition-type { cnf | dnf } [-noconfirm]**

no cscf ifc-trigger-point id *tp_id*

[no] cscf isc-template id *template_id*

CLI (CSCF IFC SPT Group Mode)

[no] spt-condition id *cond_id*

CLI (CSCF IFC Trigger Point Mode)

[no] spt-group id *group_id*

CLI (CSCF ISC Template Configuration Mode)

[no] filter-criteria id *criteria_id*

Web Element Manager Path

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

cscf peer-servers

This command creates a peer server group type for next-hop session routing and enters the Peer Server Configuration Mode. The following types of peer server groups have been added:

- **ecscf**: Emergency Call/Session Control Function
- **other**: Other Function

CLI (Context Configuration Mode)

cscf peer-servers *server_name* **type { type } [-noconfirm]**

no cscf peer-servers *server_name*

Web Element Manager Path

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

emergency

This command configures the function to allow or disallow the emergency-session or emergency-registration of a particular type. Formerly **emergency-sessions** command.

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

[default | no] emergency { registration [visited-ue] | session [3gpp-ims-xml-body | anonymous | non-emergency-registered | 3 sdp-cs-media | visited-ue]

Web Element Manager Path

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

policy

The new **accounting interim-interval** *value* keyword is used to configure Interim-Interval value for CSCF accounting sessions.

value can be configured to any integer value from 50 to 7200. This value is sent in the "Acct-Interim-Interval" AVP of the accounting message. Based on the response message from accounting server, Interim-Interval timer is started.

CLI (CSCF Service Configuration Mode)

policy { accounting interim-interval *value* **| allow-early-media | threshold congestion-control [system-cpu-utilization** *percent* **] [tolerance** *percent* **] }**

[default | no] policy { accounting interim-interval | allow-early-media | threshold congestion-control tolerance }

Web Element Manager Path

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

registration

This command configures a registration lifetime for all subscribers to the service. The maximum value has been decreased to 1209600.

CLI (CSCF Serving-CSCF Configuration Mode)

registration lifetime { default *sec* **| max** *sec* **| min** *sec* **}**

default registration lifetime

Web Element Manager Path

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

SGSN Commands - Modified in Release 11.0

The following commands have been modified in Release 11.0.

apn-selection-default

The new **`require-dns-fail-wildcard`** keyword enables the use of the default APN if the DNS query fails with the selected APN.

CLI (Exec Mode)

`apn-selection-default network-identifier` *`apn_net_id`* **`{ reject-blank-apn | require-dns-fail-wildcard | require-subscription-apn }`**

apn-selection-default

The new **`reject-blank-apn`** keyword has been added to the command to disable use of the default APN if a blank APN is received.

CLI (Exec Mode)

`apn-selection-default network-identifier` *`apn_net_id`* **`{ reject-blank-apn | require-dns-fail-wildcard | require-subscription-apn }`**

derive-imeisv-from-imei

A new keyword filter – **`derive-imeisv-from-imei`** – has been added to the **`gtp send`** command to enable the operator to configure the SGSN to send IMEI to the GGSNs an IMEI-SV.

CLI (Call-Control Profile Configuration Mode)

`gtp send { imeisv [derive-imeisv-from-imei] | ms-timezone | rat | uli }`

gtpp dictionary

Dictionaries custom31 to custom40 have been reserved. Currently, only custom31 is being used.

CLI (Context Configuration Mode)

`gtpp dictionary { custom1 | custom10 | custom11 | custom12 | custom13 | custom14 | custom15 | custom16 | custom17 | custom18 | custom19 | custom20 | custom21 | custom22 | custom23 | custom24 | custom25 | custom26 | custom27 | custom28 | custom29 | custom3 | custom30 | custom31 | custom32 | custom33 | custom34 | custom35 | custom36 | custom37 | custom38 | custom39 | custom4 | custom40 | custom5 | custom6 | custom7 | custom8 | custom9 | standard }`

max-gt-address-len

New keyword added to control the length of the mobile global title address. If used and the defined MGT string is longer, then least significant digits will be omitted during IMSI>MGT conversion.

CLI (HLR Configuration Mode)

[no] imsi { any | starts-with prefix_number } mobile-global-title mgt_number [max-gt-address-len max_gt_address]

max-gt-address-len

New keyword added to control the length of the mobile global title address. If used and the defined MGT string is longer, then least significant digits will be omitted during IMSI>MGT conversion.

CLI (SMS Service Configuration Mode)

[no] smsc-routing { any | starts-with prefix_number } mobile-global-title mgt_number [max-gt-address-len max_gt_address]

name format

A new keyword has been added to allow the format of CDR filenames to be configured independently from the file format.

CLI (GTPP Server Group Configuration Mode)

[no] gtpp storage-server local file name format *string_1-127* **[max-file-seq-no** *<1- 4294967295>* **]**

name prefix

A new value, null, has been added to the **prefix** keyword to allow the use of ‘no prefix’.

CLI (GTPP Server Group Configuration Mode)

gtpp storage-server local file name prefix

Obsoleted Commands

This section contains configuration commands that have been obsoleted in Release 11.0. Obsoleted commands in this version are divided into the following sections:

Common Commands - Obsoleted in Release 11.0

This section provides information on commands that are common to all products that were obsoleted in Release 1.0.

qos-update-timeout

This command has been obsoleted.

CLI (IMS Authorization Service Configuration Mode)

[no] qos-update-timeout *timeout-duration*

Web Element Manager Path

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

Content Filtering Commands - Obsoleted in Release 11.0

This section provides information on CF commands that were obsoleted in Release 11.0.

deny-message

This command has been obsoleted.

CLI (Content Filtering Server Group Configuration Mode)

deny-message *string*

{ default | no } deny-message

Web Element Manager Path

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

ECS Commands - Obsoleted in Release 11.0

This section provides information on ECS commands that were obsoleted in Release 11.0.

priority

This command configures the packet filter's priority. This command is deprecated in certain 9.0 releases and in 10.0 and later releases. The precedence values of packet filters (those from dynamic and predefined rules) are assigned by the PCEF based on an internal process.

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 11.0

None for this release.

GGSN Commands - Obsoleted in Release 11.0

None for this release.

HA Commands - Obsoleted in Release 11.0

None for this release.

Mobility Management Entity Commands - Obsoleted in Release 11.0

This section provides information on Mobility Management Entity (MME) commands that were obsoleted in Release 11.0.

imei-query-type

This command has been obsoleted in release 11.0 and later releases.

CLI (MME Service Configuration Mode)

`imei-query-type {none | imei | imei-sv }`

Web Element Manager Path

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

s1-mme sctp port

This command has been obsoleted in release 11.0 and later releases.

CLI (MME Service Configuration Mode)

`s1-mme sctp port` *`port`*

Web Element Manager Path

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

PDSN Commands - Obsoleted in Release 11.0

None for this release.

SGSN Commands - Obsoleted in Release 11.0

None for this release.

GTPP Storage Server (GSS)

This section provides information on GSS changes in Release 11.0.

None for this release.

Web Element Manager Changes

This section provides information on Web Element Manager changes in Release 11.0.

Enhanced Load Configuration Feature

WEM's enhanced Load Configuration feature enables users to manage all aspects of configuration file updates for systems that are accessed by an instance of the WEM.

The Load Configuration feature's user interface utilizes the structure and syntax of the ASR 5000 Command Line Interface (CLI) to provide users with the capability to efficiently duplicate, edit, create, and save configuration files and templates. Configuration files can be applied to one or more systems. Configuration templates can be created and edited to facilitate the distribution of configuration updates.

The Load Configuration feature enables authorized users to:

- Copy, create, edit, save, and apply configuration files to selected system(s).
- Use the configuration templates provided with WEM as the basis for creating and editing configuration files for deployment. Users can also create new configuration templates of their own design.
- Create Comma Separated Values (CSV) files for populating template variables with network-specific values.
- View and configure relationships between a configuration file and one or more configuration templates. This can help insure that all relevant parameter settings and values are updated before loading a configuration to a specified system.
- Apply a configuration to one or more systems. Configurations are loaded sequentially based on a user specified order. Configuration files can be loaded from a chassis, a WEM Server, a WEM Client, or other external drive. This eliminates the need for separate implementation cycles for multiple configuration updates.
- Easily isolate errors in a configuration file update. During the configuration file load operation, all errors in a configuration file being loaded are highlighted in yellow. This enables users to easily locate and resolve potential service affecting problems.
- View a currently running system's configuration file.
- Compare two configuration files or templates to identify the delta between the files.

IMPORTANT

Only WEM users with **Security Administrator** or **Config-Administrator** privileges are allowed to access and use the Load Configuration feature. In addition, to apply configuration files to one or more systems managed by an instance of the WEM, the user must have **Security Administrator** or **Config-Administrator** privileges defined on both the WEM and the system(s) being updated.

IMPORTANT

To use the Load Configuration feature, users must possess a working knowledge of the structure and syntax of the ASR 5000 CLI and be familiar with the configurations on the systems being managed by the WEM. Valid CLI commands available for use in a configuration file for a specific system are dependent on the licenses enabled and configured on the system being accessed by the WEM. Refer to the *Cisco ASR 5000 Series Command Line Interface Reference* for detailed descriptions of all commands available with the CLI.

Web Element Manager Path:

Configuration\Save/Load Configuration\Load Configuration

Support for Viewing SSC Alarm and Bulkstat Information

WEM now supports the viewing of alarm and bulkstat information for a specified Cisco Subscriber Service Controller (SSC). Users can add one or more SSCs to WEM via the NE (Network Element) List dialog box. Once the SSCs have been added, users will be able to select the SSC for viewing a variety of Alarm and Bulkstat information via the Alarm Management and Accounting menus.

IMPORTANT

Alarm and bulkstat configuration first must be performed via the SSC's Command Line Interface before that information will be available for viewing in WEM.

Web Element Manager Path:

Configuration\NE List

CHAPTER 4
ACCOUNTING MANAGEMENT

This section contains additions and changes made to the accounting-related parameters available in Release 11.0. Topics covered in this chapter are:

- *Bulk Statistic Enhancements in Release 11.0*
- *RADIUS Attributes in Release 11.0*
- *Diameter Attributes in Release 11.0*
- *Web Element Manager Enhancements*

Bulk Statistic Enhancements in Release 11.0

This section lists bulk statistic additions and changes in Release 11.0. 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*
- *Modified Bulk Statistics*
- *Obsoleted Bulk Statistics*

New Bulk Statistics

Support for the following bulk statistics were added in Release 11.0.

CSCF Schema

- emerg-regs
- mo-call-succ-rate
- mt-call-succ-rate
- mo-voice-call-succ-rate
- mt-voice-call-succ-rate
- mo-video-call-succ-rate
- mt-video-call-succ-rate
- reg-resp-439rx
- reg-resp-439tx
- rereg-resp-439rx
- rereg-resp-439tx
- message-413-rx
- message-413-tx
- rtcp-sent
- sip-tcp-subs
- msrp-active-tcp-conn
- msrp-closed-tcp-conn
- msrp-succ-tcp-conn-out
- msrp-fail-tcp-conn-out
- msrp-succ-tcp-conn-in
- msrp-fail-tcp-conn-in
- msrp-packet-rx
- msrp-packet-tx
- msrp-bytes-rx
- msrp-bytes-tx
- msrp-tcp-subs

CSCFINTF Schema

- fhloerrrx
- fhloerrtx
- mo-call-succ-rate
- mt-call-succ-rate
- mo-voice-call-succ-rate
- mt-voice-call-succ-rate
- mo-video-call-succ-rate
- mt-video-call-succ-rate

ECS Schema

- p2p-msn-non-audio-or-video-uplnk-bytes
- p2p-msn-non-audio-or-video-dwlnk-bytes
- p2p-msn-non-audio-or-video-uplnk-pkts
- p2p-msn-non-audio-or-video-dwlnk-pkts
- p2p-icecast-uplnk-bytes
- p2p-icecast-dwlnk-bytes
- p2p-icecast-uplnk-pkts
- p2p-icecast-dwlnk-pkts
- p2p-kontiki-uplnk-bytes
- p2p-kontiki-dwlnk-bytes
- p2p-kontiki-uplnk-pkts
- p2p-kontiki-dwlnk-pkts
- p2p-meebo-uplnk-bytes
- p2p-meebo-dwlnk-bytes
- p2p-meebo-uplnk-pkts
- p2p-meebo-dwlnk-pkts
- p2p-shoutcast-uplnk-bytes
- p2p-shoutcast-dwlnk-bytes
- p2p-shoutcast-uplnk-pkts
- p2p-shoutcast-dwlnk-pkts
- p2p-truphone-uplnk-bytes
- p2p-truphone-dwlnk-bytes
- p2p-truphone-uplnk-pkts
- p2p-truphone-dwlnk-pkts
- p2p-thunder-uplnk-bytes
- p2p-thunder-dwlnk-bytes
- p2p-thunder-uplnk-pkts
- p2p-thunder-dwlnk-pkts

- p2p-armagettron-uplnk-bytes
- p2p-armagettron-dwlnk-bytes
- p2p-armagettron-uplnk-pkts
- p2p-armagettron-dwlnk-pkts
- p2p-blackberry-uplnk-bytes
- p2p-blackberry-dwlnk-bytes
- p2p-blackberry-uplnk-pkts
- p2p-blackberry-dwlnk-pkts
- p2p-citrix-uplnk-bytes
- p2p-citrix-dwlnk-bytes
- p2p-citrix-uplnk-pkts
- p2p-citrix-dwlnk-pkts
- p2p-clubpenguin-uplnk-bytes
- p2p-clubpenguin-dwlnk-bytes
- p2p-clubpenguin-uplnk-pkts
- p2p-clubpenguin-dwlnk-pkts
- p2p-crossfire-uplnk-bytes
- p2p-crossfire-dwlnk-bytes
- p2p-crossfire-uplnk-pkts
- p2p-crossfire-dwlnk-pkts
- p2p-dofus-uplnk-bytes
- p2p-dofus-dwlnk-bytes
- p2p-dofus-uplnk-pkts
- p2p-dofus-dwlnk-pkts
- p2p-fiesta-uplnk-bytes
- p2p-fiesta-dwlnk-bytes
- p2p-fiesta-uplnk-pkts
- p2p-fiesta-dwlnk-pkts
- p2p-florensia-uplnk-bytes
- p2p-florensia-dwlnk-bytes
- p2p-florensia-uplnk-pkts
- p2p-florensia-dwlnk-pkts
- p2p-funshion-uplnk-bytes
- p2p-funshion-dwlnk-bytes
- p2p-funshion-uplnk-pkts
- p2p-funshion-dwlnk-pkts
- p2p-guildwars-uplnk-bytes
- p2p-guildwars-dwlnk-bytes

- p2p-guildwars-uplnk-pkts
- p2p-guildwars-dwlnk-pkts
- p2p-isakmp-uplnk-bytes
- p2p-isakmp-dwlnk-bytes
- p2p-isakmp-uplnk-pkts
- p2p-isakmp-dwlnk-pkts
- p2p-maplestory-uplnk-bytes
- p2p-maplestory-dwlnk-bytes
- p2p-maplestory-uplnk-pkts
- p2p-maplestory-dwlnk-pkts
- p2p-mgcp-uplnk-bytes
- p2p-mgcp-dwlnk-bytes
- p2p-mgcp-uplnk-pkts
- p2p-mgcp-dwlnk-pkts
- p2p-octoshape-uplnk-bytes
- p2p-octoshape-dwlnk-bytes
- p2p-octoshape-uplnk-pkts
- p2p-octoshape-dwlnk-pkts
- p2p-off-uplnk-bytes
- p2p-off-dwlnk-bytes
- p2p-off-uplnk-pkts
- p2p-off-dwlnk-pkts
- p2p-ps3-uplnk-bytes
- p2p-ps3-dwlnk-bytes
- p2p-ps3-uplnk-pkts
- p2p-ps3-dwlnk-pkts
- p2p-rmstream-uplnk-bytes
- p2p-rmstream-dwlnk-bytes
- p2p-rmstream-uplnk-pkts
- p2p-rmstream-dwlnk-pkts
- p2p-rfactor-uplnk-bytes
- p2p-rfactor-dwlnk-bytes
- p2p-rfactor-uplnk-pkts
- p2p-rfactor-dwlnk-pkts
- p2p-splashfighter-uplnk-bytes
- p2p-splashfighter-dwlnk-bytes
- p2p-splashfighter-uplnk-pkts
- p2p-splashfighter-dwlnk-pkts

- p2p-ssdp-uplnk-bytes
- p2p-ssdp-dwlnk-bytes
- p2p-ssdp-uplnk-pkts
- p2p-ssdp-dwlnk-pkts
- p2p-stealthnet-uplnk-bytes
- p2p-stealthnet-dwlnk-bytes
- p2p-stealthnet-uplnk-pkts
- p2p-stealthnet-dwlnk-pkts
- p2p-stun-uplnk-bytes
- p2p-stun-dwlnk-bytes
- p2p-stun-uplnk-pkts
- p2p-stun-dwlnk-pkts
- p2p-teamspeak-uplnk-bytes
- p2p-teamspeak-dwlnk-bytes
- p2p-teamspeak-uplnk-pkts
- p2p-teamspeak-dwlnk-pkts
- p2p-tor-uplnk-bytes
- p2p-tor-dwlnk-bytes
- p2p-tor-uplnk-pkts
- p2p-tor-dwlnk-pkts
- p2p-veohtv-uplnk-bytes
- p2p-veohtv-dwlnk-bytes
- p2p-veohtv-uplnk-pkts
- p2p-veohtv-dwlnk-pkts
- p2p-wii-uplnk-bytes
- p2p-wii-dwlnk-bytes
- p2p-wii-uplnk-pkts
- p2p-wii-dwlnk-pkts
- p2p-wmstream-uplnk-bytes
- p2p-wmstream-dwlnk-bytes
- p2p-wmstream-uplnk-pkts
- p2p-wmstream-dwlnk-pkts
- p2p-wofkungfu-uplnk-bytes
- p2p-wofkungfu-dwlnk-bytes
- p2p-wofkungfu-uplnk-pkts
- p2p-wofkungfu-dwlnk-pkts
- p2p-xdcc-uplnk-bytes
- p2p-xdcc-dwlnk-bytes

- p2p-xdcc-uplnk-pkts
- p2p-xdcc-dwlnk-pkts
- p2p-yourfreetunnel-uplnk-bytes
- p2p-yourfreetunnel-dwlnk-bytes
- p2p-yourfreetunnel-uplnk-pkts
- p2p-yourfreetunnel-dwlnk-pkts
- p2p-facebook-uplnk-bytes
- p2p-facebook-dwlnk-bytes
- p2p-facebook-uplnk-pkts
- p2p-facebook-dwlnk-pkts
- sip-advanced-calls
- sip-advanced-uplk-bytes
- sip-advanced-dwnlk-bytes
- sip-advanced-uplk-pkts
- sip-advanced-dwnlk-pkts
- sip-advanced-register-rx
- sip-advanced-invite-rx
- sip-advanced-ack-rx
- sip-advanced-bye-rx
- sip-advanced-info-rx
- sip-advanced-prack-rx
- sip-advanced-refer-rx
- sip-advanced-cancel-rx
- sip-advanced-update-rx
- sip-advanced-message-rx
- sip-advanced-options-rx
- sip-advanced-publish-rx
- sip-advanced-subscribe-rx
- sip-advanced-notify-rx
- sip-advanced-1xx-rx
- sip-advanced-2xx-rx
- sip-advanced-3xx-rx
- sip-advanced-4xx-rx
- sip-advanced-5xx-rx
- sip-advanced-6xx-rx
- sip-advanced-register-tx
- sip-advanced-invite-tx
- sip-advanced-ack-tx

- sip-advanced-bye-tx
- sip-advanced-info-tx
- sip-advanced-prack-tx
- sip-advanced-refer-tx
- sip-advanced-cancel-tx
- sip-advanced-update-tx
- sip-advanced-message-tx
- sip-advanced-options-tx
- sip-advanced-publish-tx
- sip-advanced-subscribe-tx
- sip-advanced-notify-tx
- sip-advanced-1xx-tx
- sip-advanced-2xx-tx
- sip-advanced-3xx-tx
- sip-advanced-4xx-tx
- sip-advanced-5xx-tx
- sip-advanced-6xx-tx

eGTP Schema

- tun-recv-creinddatafwdngrsp
- OutSigPktS5S8PGW
- IncSigPktS5S8PGW
- OutSigOctS5S8PGW
- IncSigOctS5S8PGW
- OutSigPktS5S8SGW
- IncSigPktS5S8SGW
- OutSigOctS5S8SGW
- IncSigOctS5S8SGW
- OutSigPktS11S4SGW
- IncSigPktS11S4SGW
- OutSigOctS11S4SGW
- IncSigOctS11S4SGW
- OutSigPktS11S10MME
- IncSigPktS11S10MME
- OutSigOctS11S10MME
- IncSigOctS11S10MME
- OutSigPktS4SGSN
- IncSigPktS4SGSN
- OutSigOctS4SGSN

- IncSigOctS4SGSN
- mobility-sent-ctxreq
- mobility-sent-retransctxreq
- mobility-recv-ctxreq
- mobility-recv-retransctxreq
- mobility-sent-ctxrsp
- mobility-sent-retransctxrsp
- mobility-recv-ctxrsp
- mobility-recv-retransctxrsp
- mobility-sent-ctxrspaccept
- mobility-sent-ctxrspdenied
- mobility-recv-ctxrspaccept
- mobility-recv-ctxrspdenied
- mobility-sent-ctxack
- mobility-sent-retransctxack
- mobility-recv-ctxack
- mobility-recv-retransctxack
- mobility-sent-ctxackaccept
- mobility-sent-ctxackdenied
- mobility-recv-ctxackaccept
- mobility-recv-ctxackdenied
- mobility-sent-idtreq
- mobility-sent-retransidtreq
- mobility-recv-idtreq
- mobility-recv-retransidtreq
- mobility-sent-idtrsp
- mobility-sent-retransidtrsp
- mobility-recv-idtrsp
- mobility-recv-retransidtrsp
- mobility-sent-idtrspaccept
- mobility-sent-idtrspdenied
- mobility-recv-idtrspaccept
- mobility-recv-idtrspdenied
- mobility-sent-fwdrelreq
- mobility-sent-retransfwdrelreq
- mobility-recv-fwdrelreq
- mobility-recv-retransfwdrelreq
- mobility-sent-fwdrelrsp

- mobility-sent-retransfwdrelrsp
- mobility-recv-fwdrelrsp
- mobility-recv-retransfwdrelrsp
- mobility-sent-fwdrelrspaccept
- mobility-sent-fwdrelrspdenied
- mobility-recv-fwdrelrspaccept
- mobility-recv-fwdrelrspdenied
- mobility-sent-fwdaccnotf
- mobility-sent-retransfwdaccnotf
- mobility-recv-fwdaccnotf
- mobility-recv-retransfwdaccnotf
- mobility-sent-fwdaccack
- mobility-sent-retransfwdaccack
- mobility-recv-fwdaccack
- mobility-recv-retransfwdaccack
- mobility-sent-fwdaccackaccept
- mobility-sent-fwdaccackdenied
- mobility-recv-fwdaccackaccept
- mobility-recv-fwdaccackdenied
- mobility-sent-fwdrelcmpnotf
- mobility-sent-retransfwdrelcmpnotf
- mobility-recv-fwdrelcmpnotf
- mobility-recv-retransfwdrelcmpnotf
- mobility-sent-fwdrelcmpack
- mobility-sent-retransfwdrelcmpack
- mobility-recv-fwdrelcmpack
- mobility-recv-retransfwdrelcmpack
- mobility-sent-fwdrelcmpackaccept
- mobility-sent-fwdrelcmpackdenied
- mobility-recv-fwdrelcmpackaccept
- mobility-recv-fwdrelcmpackdenied
- mobility-sent-relcancelreq
- mobility-sent-retransrelcancelreq
- mobility-recv-relcancelreq
- mobility-recv-retransrelcancelreq
- mobility-sent-relcancelrsp
- mobility-sent-retransrelcancelrsp
- mobility-recv-relcancelrsp

- mobility-recv-retransrelcancelrsp
- mobility-sent-relcancelrspaccept
- mobility-sent-relcancelrspdenied
- mobility-recv-relcancelrspaccept
- mobility-recv-relcancelrspdenied
- trace-sent-activate
- trace-recv-activate
- trace-sent-deactivate
- trace-recv-deactivate

HSGW Schema

The HSGW schema was added in release 11.0.

LMA Schema

- bindupd-denygrekey
- bindupd-discardrevoc
- sentrevtrig-reserved
- sentrevtrig-unspecified
- sentrevtrig-admin
- sentrevtrig-maghoffsameatt
- sentrevtrig-maghoff-unknown
- sentrevtrig-maghoff-diffatt
- sentrevtrig-perpeer
- sentrevtrig-nodelocal
- sentrevtrig-userinitsess
- sentrevtrig-accessnwsess
- sentrevtrig-ipv4hoabind
- sentrevtrig-syncbce
- sentrevtrig-unknown
- rcvdrevack-success
- rcvdrevack-partialsuccess
- revdrevack-nobinding
- rcvdrevack-noipv4hoabind
- rcvdrevack-revocnot
- rcvdrevackbindingnotidentified
- rcvdrevack-revocfailmnattch
- rcvdrevack-unknown

MAG Schema

- deniedlma-grekey
- 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
- sentrevack-success
- sentrevack-partialsuccess
- sentrevack-nobinding
- sentrevack-noipv4hoabind
- sentrevack-revocnotauth
- sentrevack-bindingnotidentified
- sentrevack-revocfailmnattch
- sentrevack-unknown

MME Schema

- servid
- sess-cur
- emmevent-assoc-attempt
- emmevent-assoc-success
- emmevent-assoc-failure
- emmevent-associmsi-attempt
- emmevent-associmsi-success
- emmevent-associmsi-failure
- emmevent-assoclocguti-attempt
- emmevent-assoclocguti-success
- emmevent-assoclocguti-failure
- emmevent-assocnonlocguti-attempt
- emmevent-assocnonlocguti-success
- emmevent-assocnonlocguti-failure

- emmevent-auth-attempt
- emmevent-auth-success
- emmevent-auth-failure
- emmevent-iden-attempt
- emmevent-iden-success
- emmevent-iden-failure
- emmevent-sec-attempt
- emmevent-sec-success
- emmevent-sec-failure
- emmevent-x2ho-attempt
- emmevent-x2ho-success
- emmevent-x2ho-failure
- emmevent-s1ho-attempt
- emmevent-s1ho-success
- emmevent-s1ho-failure
- emmevent-tau-attempt
- emmevent-tau-success
- emmevent-tau-failure
- emmevent-detach-attempt
- emmevent-detach-success
- emmevent-detach-failure
- emmevent-detachueinit-attempt
- emmevent-detachueinit-success
- emmevent-detachueinit-failure
- emmevent-detachnwinit-attempt
- emmevent-detachnwinit-success
- emmevent-detachnwinit-failure
- emmevent-detachhssinit-attempt
- emmevent-detachhssinit-success
- emmevent-detachhssinit-failure
- ecmevent-idlemode-attempt
- ecmevent-idlemode-success
- ecmevent-idlemode-failure
- ecmevent-srvcreq-attempt
- ecmevent-srvcreq-success
- ecmevent-srvcreq-failure
- ecmevent-paging-attempt
- ecmevent-paging-success

- ecmevent-paging-failure
- emmctrlmsg-sent-cleartext
- emmctrlmsg-sent-integrity
- emmctrlmsg-sent-cipher
- emmctrlmsg-sent-retrans
- emmctrlmsg-sent-failure
- emmctrlmsg-recv-cleartext
- emmctrlmsg-recv-integrity
- emmctrlmsg-recv-cipher
- emmctrlmsg-recv-accept
- emmctrlmsg-recv-discard
- emmctrlmsg-recv-denied
- emmctrlmsg-recv-deocdefail
- emmcall-attach-currcall
- emmcall-attach-maxcall
- emmcall-connect-curcall
- emmcall-connect-maxcall
- emmcall-idle-curcall
- emmcall-idle-maxcall
- emmdisc-uedetach
- emmdisc-pgwdetach
- emmdisc-hssdetach
- emmdisc-mmedetach
- emmdisc-implicitdetach
- emmdisc-localabort
- emmdisc-authfail
- emmdisc-subsparamfail
- emmdisc-otherreasons
- esmevent-pdncon-attempt
- esmevent-pdncon-success
- esmevent-pdncon-failure
- esmevent-pdndiscon-attempt
- esmevent-pdndiscon-success
- esmevent-pdndiscon-failure
- esmevent-defbearact-attempt
- esmevent-defbearact-success
- esmevent-defbearact-failure
- esmevent-dedbearact-attempt

- esmevent-dedbearact-success
- esmevent-dedbearact-failure
- esmevent-beardeact-attempt
- esmevent-beardeact-success
- esmevent-beardeact-failure
- esmctrlmsg-sent-cleartext
- esmctrlmsg-sent-integrity
- esmctrlmsg-sent-cipher
- esmctrlmsg-sent-retrans
- esmctrlmsg-sent-failure
- esmctrlmsg-recv-cleartext
- esmctrlmsg-recv-integrity
- esmctrlmsg-recv-cipher
- esmctrlmsg-recv-accept
- esmctrlmsg-recv-discard
- esmctrlmsg-recv-denied
- esmctrlmsg-recv-deocdefail
- sctp-transdata-init
- sctp-transdata-initack
- sctp-transdata-shut
- sctp-transdata-shutack
- sctp-transdata-cookie
- sctp-transdata-cookieack
- sctp-transdata-data
- sctp-transdata-dataack
- sctp-transdata-shutcomp
- sctp-transdata-hb
- sctp-transdata-hback
- sctp-transdata-abort
- sctp-transdata-error
- sctp-recdata-init
- sctp-recdata-initack
- sctp-recdata-shut
- sctp-recdata-shutack
- sctp-recdata-cookie
- sctp-recdata-cookieack
- sctp-recdata-data
- sctp-recdata-dataack

- sctp-recdata-shutcomp
- sctp-recdata-hb
- sctp-recdata-hback
- sctp-recdata-abort
- sctp-recdata-error
- sctp-retransdata-init
- sctp-retransdata-shut
- sctp-retransdata-shutack
- sctp-retransdata-cookie
- sctp-retransdata-cookieack
- sctp-totsent-bytes
- sctp-totrec-bytes
- sctp-totsent-pkts
- sctp-totrec-pkts
- s1ap-transdata-setupres
- s1ap-transdata-setupresfail
- s1ap-transdata-reset
- s1ap-transdata-resetack
- s1ap-transdata-olstart
- s1ap-transdata-olstop
- s1ap-transdata-mmedirinftra
- s1ap-transdata-paging
- s1ap-transdata-enbcfgupdack
- s1ap-transdata-enbcfgupdfail
- s1ap-transdata-ctrlmsgencfail
- s1ap-transdata-erabsetupreq
- s1ap-transdata-erabmodreq
- s1ap-transdata-erabrelcmd
- s1ap-transdata-ctxtsetupreq
- s1ap-transdata-uectxtrel
- s1ap-transdata-uectxtmod
- s1ap-transdata-dlnastrans
- s1ap-transdata-errorind
- s1ap-transdata-hocmd
- s1ap-transdata-hoprepfail
- s1ap-transdata-horeq
- s1ap-transdata-hocanack
- s1ap-transdata-pathswreqack

- s1ap-transdata-pathswreqfail
- s1ap-transdata-dlinktunnel
- s1ap-transdata-tracestart
- s1ap-transdata-deactivtrace
- s1ap-transdata-mmetrans
- s1ap-transdata-locrepctrl
- s1ap-transdata-encfail
- s1ap-recdata-setupreq
- s1ap-recdata-reset
- s1ap-recdata-resetack
- s1ap-recdata-enbdirinftrans
- s1ap-recdata-enbcfgupd
- s1ap-recdata-ctrlmsgdecfail
- s1ap-recdata-ctrlmsgunexpevt
- s1ap-recdata-erabsetupres
- s1ap-recdata-erabmodres
- s1ap-recdata-erabrelres
- s1ap-recdata-erabrelind
- s1ap-recdata-ctxtsetupres
- s1ap-recdata-ctxtsetupfail
- s1ap-recdata-uectxtrelreq
- s1ap-recdata-uectxtrelcomp
- s1ap-recdata-uectxtmodres
- s1ap-recdata-uectxtmodfail
- s1ap-recdata-inituemsg
- s1ap-recdata-ulinknastp
- s1ap-recdata-nasnondelind
- s1ap-recdata-errorind
- s1ap-recdata-horeqack
- s1ap-recdata-hocancel
- s1ap-recdata-horequire
- s1ap-recdata-hofail
- s1ap-recdata-honotify
- s1ap-recdata-pathswreq
- s1ap-recdata-enbstatustrans
- s1ap-recdata-uecap
- s1ap-recdata-ulinktunnel
- s1ap-recdata-tracefailind

- s1ap-recdata-locrep
- s1ap-recdata-locrepfailind
- s1ap-recdata-decfail
- s1ap-recdata-unexpevt
- emmevent-tauattach-success
- emmevent-tauattach-failure
- emmevent-outrauho4g3g-success
- emmevent-outrauho4g3g-failure
- emmevent-outs1ho4g3g-success
- emmevent-outs1ho4g3g-failure
- emmevent-intauho3g4g-success
- emmevent-intauho3g4g-failure
- emmevent-ins1ho3g4g-success
- emmevent-ins1ho3g4g-failure
- epsattach-imsi-attempted
- epsattach-imsi-success
- epsattach-imsi-failures
- epsattach-guti-local-attempted
- epsattach-guti-local-success
- epsattach-guti-local-failures
- epsattach-guti-foreign-attempted
- epsattach-guti-foreign-success
- epsattach-guti-foreign-failures
- epsattach-ptmsi-attempted
- epsattach-ptmsi-success
- epsattach-ptmsi-failures
- epstauattach-guti-foreign-attempted
- epstauattach-guti-foreign-success
- epstauattach-guti-foreign-failures
- epstauattach-ptmsi-attempted
- epstauattach-ptmsi-success
- epstauattach-ptmsi-failures
- combinedattach-imsi-attempted
- combinedattach-imsi-success
- combinedattach-imsi-success-eps
- combinedattach-imsi-failure
- combinedattach-guti-local-attached
- combinedattach-guti-local-success

- combinedattach-guti-local-success-eps
- combinedattach-guti-local-failure
- combinedattach-guti-foreign-attempted
- combinedattach-guti-foreign-success
- combinedattach-guti-foreign-success-eps
- combinedattach-guti-foreign-failure
- combinedattach-ptmsi-attempted
- combinedattach-ptmsi-success
- combinedattach-ptmsi-success-eps
- combinedattach-ptmsi-failure
- combined-tauattach-guti-foreign-attempted
- combined-tauattach-guti-foreign-success
- combined-tauattach-guti-foreign-success-eps
- combined-tauattach-guti-foreign-failure
- combined-tauattach-ptmsi-attempted
- combined-tauattach-ptmsi-success
- combined-tauattach-ptmsi-success-eps
- combined-tauattach-ptmsi-failure
- tau-periodic-attempted
- tau-periodic-success
- tau-periodic-failures
- tau-normal-attempted
- tau-normal-success
- tau-normal-failures
- tau-active-attempted
- tau-active-success
- tau-active-failures
- tau-sgw-change-attempted
- tau-sgw-change-success
- tau-sgw-change-failures
- paging-init-events-attempted
- paging-init-events-success
- paging-init-events-failures
- paging-last-enb-success
- paging-last-tai-success
- emm-msgtx-attach-accept
- emm-msgtx-attach-accept-retx
- emm-msgtx-attach-reject

- emm-msgtx-imsi-unknown-hss
- emm-msgtx-illegal-ue
- emm-msgtx-illegal-me
- emm-msgtx-eps-not-allowed
- emm-msgtx-network-failure
- emm-msgtx-esm-failure
- emm-msgtx-decode-failure
- emm-msgtx-auth-reject
- emm-msgtx-auth-req
- emm-msgtx-auth-req-retx
- emm-msgtx-detach-request
- emm-msgtx-detach-req-retx
- emm-msgtx-reattach-req
- emm-msgtx-rettach-not-req
- emm-msgtx-imsi-detach
- emm-msgtx-detach-accept
- emm-msgtx-downlink-transport
- emm-msgtx-emm-info
- emm-msgtx-emm-status
- emm-msgtx-guti-reloc
- emm-msgtx-guti-reloc-retx
- emm-msgtx-identity-req
- emm-msgtx-identity-req-retx
- emm-msgtx-sm-cmd
- emm-msgtx-sm-cmd-retx
- emm-msgtx-service-reject
- emm-msgtx-ue-identity-unk
- emm-msgtx-impl-detached
- emm-msgtx-tau-accept
- emm-msgtx-tau-accept-retx
- emm-msgtx-tau-reject
- emm-msgtx-tau-imsi-unknown-hss
- emm-msgtx-tau-illegal-ue
- emm-msgtx-tau-illegal-me
- emm-msgtx-tau-eps-not-allowed
- emm-msgtx-tau-network-fail
- emm-msgtx-tau-esm-failure
- emm-msgtx-tau-decode-failure

- emm-msgtx-tau-no-bearer-active
- emm-msgtx-tau-ue-identity-unk
- emm-msgtx-tau-implicit-detached
- emm-msgrx-plain-nas
- emm-msgrx-integrity
- emm-msgrx-ciphered
- emm-msgrx-accepted
- emm-msgrx-discarded
- emm-msgrx-denied
- emm-msgrx-decode-failure
- emm-msgrx-attach-complete
- emm-msgrx-attach-req
- emm-msgrx-attach-retx
- emm-msgrx-auth-failure
- emm-msgrx-auth-resp
- emm-msgrx-detach-req
- emm-msgrx-detach-req-switchoff
- emm-msgrx-detach-req-not-switchoff
- emm-msgrx-imsi-detach
- emm-msgrx-emm-status
- emm-msgrx-guti-reloc-complete
- emm-msgrx-sm-complete
- emm-msgrx-sm-reject
- emm-msgrx-service-req
- emm-msgrx-tau-req
- emm-msgrx-tau-retx
- emm-msgrx-tau-complete
- pdn-disconnect-ue-attempted
- pdn-disconnect-ue-success
- pdn-disconnect-ue-failures
- pdn-disconnect-mme-attempted
- pdn-disconnect-mme-success
- pdn-disconnect-mme-failures
- pdn-disconnect-pgw-attempted
- pdn-disconnect-pgw-success
- pdn-disconnect-pgw-failures
- pdn-disconnect-hss-attempted
- pdn-disconnect-hss-success

- pdn-disconnect-hss-failures
- dedi-brr-activation-ue-attempted
- dedi-brr-activation-ue-success
- dedi-brr-activation-ue-failures
- brr-deactivation-mme-attempted
- brr-deactivation-mme-success
- brr-deactivation-mme-failures
- brr-deactivation-pgw-attempted
- brr-deactivation-pgw-success
- brr-deactivation-pgw-failures
- brr-deactivation-ue-attempted
- brr-deactivation-ue-success
- brr-deactivation-ue-failures
- brr-modification-hss-attempted
- brr-modification-hss-success
- brr-modification-hss-failures
- brr-modification-pgw-attemted
- brr-modification-pgw-success
- brr-modification-pgw-failures
- brr-modification-ue-attempted
- brr-modification-ue-success
- brr-modification-ue-failures
- esm-msgtx-act-ded-brr
- esm-msgtx-act-ded-brr-retx
- esm-msgtx-act-dflt-brr
- esm-msgtx-act-dflt_bee-retx
- esm-msgtx-brralloc-rej
- esm-msgtx-brralloc-rej-pt1-inuse
- esm-msgtx-brralloc-rej-semantic-errtft
- esm-msgtx-brralloc-rej-syntactic-errtft
- esm-msgtx-brralloc-rej-invalid-brrid
- esm-msgtx-brralloc-rej-collision-nwop
- esm-msgtx-brralloc-rej-pgw-rej
- esm-msgtx-brralloc-rej-invalid-pti
- esm-msgtx-brrmod-rej
- esm-msgtx-brrmod-rej-pti-inuse
- esm-msgtx-brrmod-rej-semantic-errtft
- esm-msgtx-brrmod-rej-syntactic-errtft

- esm-msgtx-brrmod-rej-invalid-brrid
- esm-msgtx-brrmod-rej-collision-nwop
- esm-msgtx-brrmod-rej-pgw-rej
- esm-msgtx-brrmod-rej-invalid-pti
- esm-msgtx-deactbrr
- esm-msgtx-deactbrr-retx
- esm-msgtx-deactbrr-esm-info-req
- esm-msgtx-deactbrr-esm-info-req-retx
- esm-msgtx-deactbrr-modbrr
- esm-msgtx-deactbrr-moderr-retx
- esm-msgtx-pdncon-rej
- esm-msgtx-pdncon-rej-pti-inuse
- esm-msgtx-pdncon-rej-apn-unk
- esm-msgtx-pdncon-rej-pdntype-unk
- esm-msgtx-pdncon-rej-inv-brrid
- esm-msgtx-pdncon-rej-inv-pti
- esm-msgtx-pdncon-rej-pgw-rej
- esm-msgtx-pdndiscon-rej
- esm-msgtx-pdndiscon-rej-pti-inuse
- esm-msgtx-pdndiscon-rej-lastpdn
- esm-msgtx-pdndiscon-rej-inv-pti
- esm-msgtx-pdndiscon-rej-inv-brrid
- esm-msgtx-pdndiscon-rej-pgw-rej
- esm-msgrx-plain-nas
- esm-msgrx-integrity
- esm-msgrx-ciphered
- esm-msgrx-accepted
- esm-msgrx-discarded
- esm-msgrx-denied
- esm-msgrx-decode-failures
- esm-msgrx-ded-brr-accept
- esm-msgrx-ded-brr-reject
- esm-msgrx-dflt-brr-accept
- esm-msgrx-dflt-brr-reject
- esm-msgrx-brr-rsrc-alloc-req
- esm-msgrx-brr-rsrc-modify-req
- esm-msgrx-esm-info-resp
- esm-msgrx-em-status

- esm-msgrx-mod-brr-accept
- esm-msgrx-mod-brr-reject
- esm-msgrx-pdn-con-req
- esm-msgrx-pdn-discon-req
- out-tau-ho-4gto4g-s10-attempted
- out-tau-ho-4gto4g-s10-success
- out-tau-ho-4gto4g-s10-failures
- out-s1-ho-4gto4g-s10-attempted
- out-s1-ho-4gto4g-s10-success
- out-s1-ho-4gto4g-s10-failures
- in-tau-ho-4gto4g-s10-attempted
- in-tau-ho-4gto4g-s10-success
- in-tau-ho-4gto4g-s10-failures
- in-s1-ho-4gto4g-s10-attempted
- in-s1-ho-4gto4g-s10-success
- in-s1-ho-4gto4g-s10-failures
- out-rau-ho-4gto3g-gngp-attempted
- out-rau-ho-4gto3g-gngp-success
- out-rau-ho-4gto3g-gngp-failures
- out-s1-ho-4gto3g-gngp-attempted
- out-s1-ho-4gto3g-gngp-success
- out-s1-ho-4gto3g-gngp-failures
- in-tau-ho-3gto4g-gngp-attempted
- in-tau-ho-3gto4g-gngp-success
- in-tau-ho-3gto4g-gngp-failures
- in-s1-ho-3gto4g-gngp-attempted
- in-s1-ho-3gto4g-gngp-success
- in-s1-ho-3gto4g-gngp-failures
- out-rau-ho-4gto2g-gngp-attempted
- out-rau-ho-4gto2g-gngp-success
- out-rau-ho-4gto2g-gngp-failures
- out-s1-ho-4gto2g-gngp-attempted
- out-s1-ho-4gto2g-gngp-success
- out-s1-ho-4gto2g-gngp-failures
- in-tau-ho-2gto4g-gngp-attempted
- in-tau-ho-2gto4g-gngp-success
- in-tau-ho-2gto4g-gngp-failures
- in-s1-ho-2gto4g-gngp-attempted

- in-s1-ho-2gto4g-gngp-success
- in-s1-ho-2gto4g-gngp-failures
- tot-pdn-current
- tot-pdn-max
- connected-pdn-current
- connected-pdn-max
- idle-pdn-current
- idle-pdn-max
- tot-brr-current
- tot-brr-max
- connected-brr-current
- connected-brr-max
- idle-brr-current
- idle-brr-max

PGW Schema

- sessstat-nw-init-no-qos-update-att

PPP Schema

- ipv6cp-fail-maxretry
- ipv6cp-fail-optiss
- ipv6cp-fail-unknown
- entered-ipv6cp
- timeout-toplus
- disc-ipv6cp-excretry
- disc-ipv6cp-optnegfail
- eap-authattempt
- eap-authsuccess
- eap-authfail
- eap-authabort
- vsncp-err-gen
- vsncp-err-unauthapn
- vsncp-err-pdnlimit
- vsncp-err-nopdngw
- vsncp-err-pdngwunreach
- vsncp-err-pdngwrej
- vsncp-err-insufparam
- vsncp-err-resunava
- vsncp-err-admpro

- vsncp-err-pdniduse
- vsncp-err-sublimit
- vsncp-err-pdnexist

SGSN Schema

- ps-inter-rat-rau-fail-3g
- comb-inter-rat-rau-fail-3g
- comb-inter-rat-rau-fail-2g
- ps-inter-service-rau-fail-3g
- ps-inter-service-rau-fail-2g
- comb-inter-service-rau-fail-3g
- comb-inter-service-rau-fail-2g

S-GW Schema

- sessstat-pdnrelrsn-s4err
- sessstat-pdnrelrsn-s12err
- sessstat-pdnrelrsn-pathfail-S4
- sessstat-pdnrelrsn-pathfail-S12
- sessstat-pdnrelrsn-pathfail-S4-u
- totepsbearrel-dedrsn-s4err
- totepsbearrel-dedrsn-s12err
- totepsbearrel-dedrsn-pathfail-s12
- totepsbearrel-dedrsn-pathfail-s4-u
- intersgwhaovstat-pdnin-x2-success
- intersgwhaovstat-pdnin-x2-fail
- intersgwhaovstat-pdnin-idletau-success
- intersgwhaovstat-pdnin-idletau-fail
- intersgwhaovstat-pdnin-s1-success
- intersgwhaovstat-pdnin-s1-fail
- intrasgwhaovstat-intramme-success
- intrasgwhaovstat-intramme-fail
- intrasgwhaovstat-intermme-success
- intrasgwhaovstat-intermme-fail
- intersgwhaovstat-intersystem
- intersgwhaovstat-intersystem-success
- intersgwhaovstat-intersystem-fail
- intrasgwhaovstat-intrasgsn
- intrasgwhaovstat-intrasgsn-success
- intrasgwhaovstat-intrasgsn-fail

- intrasgwhaovstat-intersgsn
- intrasgwhaovstat-intersgsn-success
- intrasgwhaovstat-intersgsn-fail
- intrasgwhaovstat-mme-to-sgsn
- intrasgwhaovstat-mme-to-sgsn-success
- intrasgwhaovstat-mme-to-sgsn-fail
- intrasgwhaovstat-sgsn-to-mme
- intrasgwhaovstat-sgsn-to-mme-success
- intrasgwhaovstat-sgsn-to-mme-fail
- plmnstat-home-pdn-active
- plmnstat-home-pdn-setup
- plmnstat-home-pdn-released
- plmnstat-roam-pdn-active
- plmnstat-roam-pdn-setup
- plmnstat-roam-pdn-released
- plmnstat-vist-pdn-active
- plmnstat-vist-pdn-setup
- plmnstat-vist-pdn-released
- srcviolatestat-packets-dropped
- srcviolatestat-bytes-dropped
- s1u-uplnk-packets
- s1u-uplnk-bytes
- s1u-downlnk-packets
- s1u-downlnk-bytes
- s1u-uplnk-dropped-packets
- s1u-uplnk-dropped-bytes
- s1u-downlnk-dropped-packets
- s1u-downlnk-dropped-bytes
- s1u-uplnk-qci1totbyte
- s1u-uplnk-qci1totpkt
- s1u-uplnk-qci2totbyte
- s1u-uplnk-qci2totpkt
- s1u-uplnk-qci3totbyte
- s1u-uplnk-qci3totpkt
- s1u-uplnk-qci4totbyte
- s1u-uplnk-qci4totpkt
- s1u-uplnk-qci5totbyte
- s1u-uplnk-qci5totpkt

- s1u-uplnk-qci6totbyte
- s1u-uplnk-qci6totpkt
- s1u-uplnk-qci7totbyte
- s1u-uplnk-qci7totpkt
- s1u-uplnk-qci8totbyte
- s1u-uplnk-qci8totpkt
- s1u-uplnk-qci9totbyte
- s1u-uplnk-qci9totpkt
- s1u-uplnk-othertotbyte
- s1u-uplnk-othertotpkt
- s1u-uplnk-drop-qci1totbyte
- s1u-uplnk-drop-qci1totpkt
- s1u-uplnk-drop-qci2totbyte
- s1u-uplnk-drop-qci2totpkt
- s1u-uplnk-drop-qci3totbyte
- s1u-uplnk-drop-qci3totpkt
- s1u-uplnk-drop-qci4totbyte
- s1u-uplnk-drop-qci4totpkt
- s1u-uplnk-drop-qci5totbyte
- s1u-uplnk-drop-qci5totpkt
- s1u-uplnk-drop-qci6totbyte
- s1u-uplnk-drop-qci6totpkt
- s1u-uplnk-drop-qci7totbyte
- s1u-uplnk-drop-qci7totpkt
- s1u-uplnk-drop-qci8totbyte
- s1u-uplnk-drop-qci8totpkt
- s1u-uplnk-drop-qci9totbyte
- s1u-uplnk-drop-qci9totpkt
- s1u-uplnk-drop-othertotbyte
- s1u-uplnk-drop-otherpkt
- s1u-downlnk-qci1totbyte
- s1u-downlnk-qci1totpkt
- s1u-downlnk-qci2totbyte
- s1u-downlnk-qci2totpkt
- s1u-downlnk-qci3totbyte
- s1u-downlnk-qci3totpkt
- s1u-downlnk-qci4totbyte
- s1u-downlnk-qci4totpkt

- s1u-downlnk-qci5totbyte
- s1u-downlnk-qci5totpkt
- s1u-downlnk-qci6totbyte
- s1u-downlnk-qci6totpkt
- s1u-downlnk-qci7totbyte
- s1u-downlnk-qci7totpkt
- s1u-downlnk-qci8totbyte
- s1u-downlnk-qci8totpkt
- s1u-downlnk-qci9totbyte
- s1u-downlnk-qci9totpkt
- s1u-downlnk-othertotbyte
- s1u-downlnk-othertotpkt
- s1u-downlnk-drop-qci1totbyte
- s1u-downlnk-drop-qci1totpkt
- s1u-downlnk-drop-qci2totbyte
- s1u-downlnk-drop-qci2totpkt
- s1u-downlnk-drop-qci3totbyte
- s1u-downlnk-drop-qci3totpkt
- s1u-downlnk-drop-qci4totbyte
- s1u-downlnk-drop-qci4totpkt
- s1u-downlnk-drop-qci5totbyte
- s1u-downlnk-drop-qci5totpkt
- s1u-downlnk-drop-qci6totbyte
- s1u-downlnk-drop-qci6totpkt
- s1u-downlnk-drop-qci7totbyte
- s1u-downlnk-drop-qci7totpkt
- s1u-downlnk-drop-qci8totbyte
- s1u-downlnk-drop-qci8totpkt
- s1u-downlnk-drop-qci9totbyte
- s1u-downlnk-drop-qci9totpkt
- s1u-downlnk-drop-othertotbyte
- s1u-downlnk-drop-othertotpkt
- s4u-uplnk-packets
- s4u-uplnk-bytes
- s4u-downlnk-packets
- s4u-downlnk-bytes
- s4u-uplnk-dropped-packets
- s4u-uplnk-dropped-bytes

- s4u-downlnk-dropped-packets
- s4u-downlnk-dropped-bytes
- s4u-uplnk-qci1totbyte
- s4u-uplnk-qci1totpkt
- s4u-uplnk-qci2totbyte
- s4u-uplnk-qci2totpkt
- s4u-uplnk-qci3totbyte
- s4u-uplnk-qci3totpkt
- s4u-uplnk-qci4totbyte
- s4u-uplnk-qci4totpkt
- s4u-uplnk-qci5totbyte
- s4u-uplnk-qci5totpkt
- s4u-uplnk-qci6totbyte
- s4u-uplnk-qci6totpkt
- s4u-uplnk-qci7totbyte
- s4u-uplnk-qci7totpkt
- s4u-uplnk-qci8totbyte
- s4u-uplnk-qci8totpkt
- s4u-uplnk-qci9totbyte
- s4u-uplnk-qci9totpkt
- s4u-uplnk-othertotbyte
- s4u-uplnk-othertotpkt
- s4u-uplnk-drop-qci1totbyte
- s4u-uplnk-drop-qci1totpkt
- s4u-uplnk-drop-qci2totbyte
- s4u-uplnk-drop-qci2totpkt
- s4u-uplnk-drop-qci3totbyte
- s4u-uplnk-drop-qci3totpkt
- s4u-uplnk-drop-qci4totbyte
- s4u-uplnk-drop-qci4totpkt
- s4u-uplnk-drop-qci5totbyte
- s4u-uplnk-drop-qci5totpkt
- s4u-uplnk-drop-qci6totbyte
- s4u-uplnk-drop-qci6totpkt
- s4u-uplnk-drop-qci7totbyte
- s4u-uplnk-drop-qci7totpkt
- s4u-uplnk-drop-qci8totbyte
- s4u-uplnk-drop-qci8totpkt

- s4u-uplnk-drop-qci9totbyte
- s4u-uplnk-drop-qci9totpkt
- s4u-uplnk-drop-othertotbyte
- s4u-uplnk-drop-otherpkt
- s4u-downlnk-qci1totbyte
- s4u-downlnk-qci1totpkt
- s4u-downlnk-qci2totbyte
- s4u-downlnk-qci2totpkt
- s4u-downlnk-qci3totbyte
- s4u-downlnk-qci3totpkt
- s4u-downlnk-qci4totbyte
- s4u-downlnk-qci4totpkt
- s4u-downlnk-qci5totbyte
- s4u-downlnk-qci5totpkt
- s4u-downlnk-qci6totbyte
- s4u-downlnk-qci6totpkt
- s4u-downlnk-qci7totbyte
- s4u-downlnk-qci7totpkt
- s4u-downlnk-qci8totbyte
- s4u-downlnk-qci8totpkt
- s4u-downlnk-qci9totbyte
- s4u-downlnk-qci9totpkt
- s4u-downlnk-othertotbyte
- s4u-downlnk-othertotpkt
- s4u-downlnk-drop-qci1totbyte
- s4u-downlnk-drop-qci1totpkt
- s4u-downlnk-drop-qci2totbyte
- s4u-downlnk-drop-qci2totpkt
- s4u-downlnk-drop-qci3totbyte
- s4u-downlnk-drop-qci3totpkt
- s4u-downlnk-drop-qci4totbyte
- s4u-downlnk-drop-qci4totpkt
- s4u-downlnk-drop-qci5totbyte
- s4u-downlnk-drop-qci5totpkt
- s4u-downlnk-drop-qci6totbyte
- s4u-downlnk-drop-qci6totpkt
- s4u-downlnk-drop-qci7totbyte
- s4u-downlnk-drop-qci7totpkt

- s4u-downlnk-drop-qci8totbyte
- s4u-downlnk-drop-qci8totpkt
- s4u-downlnk-drop-qci9totbyte
- s4u-downlnk-drop-qci9totpkt
- s4u-downlnk-drop-othertotbyte
- s4u-downlnk-drop-othertotpkt
- s12-uplnk-packets
- s12-uplnk-bytes
- s12-downlnk-packets
- s12-downlnk-bytes
- s12-uplnk-dropped-packets
- s12-uplnk-dropped-bytes
- s12-downlnk-dropped-packets
- s12-downlnk-dropped-bytes
- s12-uplnk-qci1totbyte
- s12-uplnk-qci1totpkt
- s12-uplnk-qci2totbyte
- s12-uplnk-qci2totpkt
- s12-uplnk-qci3totbyte
- s12-uplnk-qci3totpkt
- s12-uplnk-qci4totbyte
- s12-uplnk-qci4totpkt
- s12-uplnk-qci5totbyte
- s12-uplnk-qci5totpkt
- s12-uplnk-qci6totbyte
- s12-uplnk-qci6totpkt
- s12-uplnk-qci7totbyte
- s12-uplnk-qci7totpkt
- s12-uplnk-qci8totbyte
- s12-uplnk-qci8totpkt
- s12-uplnk-qci9totbyte
- s12-uplnk-qci9totpkt
- s12-uplnk-othertotbyte
- s12-uplnk-othertotpkt
- s12-uplnk-drop-qci1totbyte
- s12-uplnk-drop-qci1totpkt
- s12-uplnk-drop-qci2totbyte
- s12-uplnk-drop-qci2totpkt

- s12-uplnk-drop-qci3totbyte
- s12-uplnk-drop-qci3totpkt
- s12-uplnk-drop-qci4totbyte
- s12-uplnk-drop-qci4totpkt
- s12-uplnk-drop-qci5totbyte
- s12-uplnk-drop-qci5totpkt
- s12-uplnk-drop-qci6totbyte
- s12-uplnk-drop-qci6totpkt
- s12-uplnk-drop-qci7totbyte
- s12-uplnk-drop-qci7totpkt
- s12-uplnk-drop-qci8totbyte
- s12-uplnk-drop-qci8totpkt
- s12-uplnk-drop-qci9totbyte
- s12-uplnk-drop-qci9totpkt
- s12-uplnk-drop-othertotbyte
- s12-uplnk-drop-otherpkt
- s12-downlnk-qci1totbyte
- s12-downlnk-qci1totpkt
- s12-downlnk-qci2totbyte
- s12-downlnk-qci2totpkt
- s12-downlnk-qci3totbyte
- s12-downlnk-qci3totpkt
- s12-downlnk-qci4totbyte
- s12-downlnk-qci4totpkt
- s12-downlnk-qci5totbyte
- s12-downlnk-qci5totpkt
- s12-downlnk-qci6totbyte
- s12-downlnk-qci6totpkt
- s12-downlnk-qci7totbyte
- s12-downlnk-qci7totpkt
- s12-downlnk-qci8totbyte
- s12-downlnk-qci8totpkt
- s12-downlnk-qci9totbyte
- s12-downlnk-qci9totpkt
- s12-downlnk-othertotbyte
- s12-downlnk-othertotpkt
- s12-downlnk-drop-qci1totbyte
- s12-downlnk-drop-qci1totpkt

- s12-downlnk-drop-qci2totbyte
- s12-downlnk-drop-qci2totpkt
- s12-downlnk-drop-qci3totbyte
- s12-downlnk-drop-qci3totpkt
- s12-downlnk-drop-qci4totbyte
- s12-downlnk-drop-qci4totpkt
- s12-downlnk-drop-qci5totbyte
- s12-downlnk-drop-qci5totpkt
- s12-downlnk-drop-qci6totbyte
- s12-downlnk-drop-qci6totpkt
- s12-downlnk-drop-qci7totbyte
- s12-downlnk-drop-qci7totpkt
- s12-downlnk-drop-qci8totbyte
- s12-downlnk-drop-qci8totpkt
- s12-downlnk-drop-qci9totbyte
- s12-downlnk-drop-qci9totpkt
- s12-downlnk-drop-othertotbyte
- s12-downlnk-drop-othertotpkt
- s5-uplnk-packets
- s5-uplnk-bytes
- s5-downlnk-packets
- s5-downlnk-bytes
- s5-uplnk-dropped-packets
- s5-uplnk-dropped-bytes
- s5-downlnk-dropped-packets
- s5-downlnk-dropped-bytes
- s5-uplnk-qci1totbyte
- s5-uplnk-qci1totpkt
- s5-uplnk-qci2totbyte
- s5-uplnk-qci2totpkt
- s5-uplnk-qci3totbyte
- s5-uplnk-qci3totpkt
- s5-uplnk-qci4totbyte
- s5-uplnk-qci4totpkt
- s5-uplnk-qci5totbyte
- s5-uplnk-qci5totpkt
- s5-uplnk-qci6totbyte
- s5-uplnk-qci6totpkt

- s5-uplnk-qci7totbyte
- s5-uplnk-qci7totpkt
- s5-uplnk-qci8totbyte
- s5-uplnk-qci8totpkt
- s5-uplnk-qci9totbyte
- s5-uplnk-qci9totpkt
- s5-uplnk-othertotbyte
- s5-uplnk-othertotpkt
- s5-uplnk-drop-qci1totbyte
- s5-uplnk-drop-qci1totpkt
- s5-uplnk-drop-qci2totbyte
- s5-uplnk-drop-qci2totpkt
- s5-uplnk-drop-qci3totbyte
- s5-uplnk-drop-qci3totpkt
- s5-uplnk-drop-qci4totbyte
- s5-uplnk-drop-qci4totpkt
- s5-uplnk-drop-qci5totbyte
- s5-uplnk-drop-qci5totpkt
- s5-uplnk-drop-qci6totbyte
- s5-uplnk-drop-qci6totpkt
- s5-uplnk-drop-qci7totbyte
- s5-uplnk-drop-qci7totpkt
- s5-uplnk-drop-qci8totbyte
- s5-uplnk-drop-qci8totpkt
- s5-uplnk-drop-qci9totbyte
- s5-uplnk-drop-qci9totpkt
- s5-uplnk-drop-othertotbyte
- s5-uplnk-drop-otherpkt
- s5-downlnk-qci1totbyte
- s5-downlnk-qci1totpkt
- s5-downlnk-qci2totbyte
- s5-downlnk-qci2totpkt
- s5-downlnk-qci3totbyte
- s5-downlnk-qci3totpkt
- s5-downlnk-qci4totbyte
- s5-downlnk-qci4totpkt
- s5-downlnk-qci5totbyte
- s5-downlnk-qci5totpkt

- s5-downlnk-qci6totbyte
- s5-downlnk-qci6totpkt
- s5-downlnk-qci7totbyte
- s5-downlnk-qci7totpkt
- s5-downlnk-qci8totbyte
- s5-downlnk-qci8totpkt
- s5-downlnk-qci9totbyte
- s5-downlnk-qci9totpkt
- s5-downlnk-othertotbyte
- s5-downlnk-othertotpkt
- s5-downlnk-drop-qci1totbyte
- s5-downlnk-drop-qci1totpkt
- s5-downlnk-drop-qci2totbyte
- s5-downlnk-drop-qci2totpkt
- s5-downlnk-drop-qci3totbyte
- s5-downlnk-drop-qci3totpkt
- s5-downlnk-drop-qci4totbyte
- s5-downlnk-drop-qci4totpkt
- s5-downlnk-drop-qci5totbyte
- s5-downlnk-drop-qci5totpkt
- s5-downlnk-drop-qci6totbyte
- s5-downlnk-drop-qci6totpkt
- s5-downlnk-drop-qci7totbyte
- s5-downlnk-drop-qci7totpkt
- s5-downlnk-drop-qci8totbyte
- s5-downlnk-drop-qci8totpkt
- s5-downlnk-drop-qci9totbyte
- s5-downlnk-drop-qci9totpkt
- s5-downlnk-drop-othertotbyte
- s5-downlnk-drop-othertotpkt
- s8-uplnk-packets
- s8-uplnk-bytes
- s8-downlnk-packets
- s8-downlnk-bytes
- s8-uplnk-dropped-packets
- s8-uplnk-dropped-bytes
- s8-downlnk-dropped-packets
- s8-downlnk-dropped-bytes

- s8-uplnk-qci1totbyte
- s8-uplnk-qci1totpkt
- s8-uplnk-qci2totbyte
- s8-uplnk-qci2totpkt
- s8-uplnk-qci3totbyte
- s8-uplnk-qci3totpkt
- s8-uplnk-qci4totbyte
- s8-uplnk-qci4totpkt
- s8-uplnk-qci5totbyte
- s8-uplnk-qci5totpkt
- s8-uplnk-qci6totbyte
- s8-uplnk-qci6totpkt
- s8-uplnk-qci7totbyte
- s8-uplnk-qci7totpkt
- s8-uplnk-qci8totbyte
- s8-uplnk-qci8totpkt
- s8-uplnk-qci9totbyte
- s8-uplnk-qci9totpkt
- s8-uplnk-othertotbyte
- s8-uplnk-othertotpkt
- s8-uplnk-drop-qci1totbyte
- s8-uplnk-drop-qci1totpkt
- s8-uplnk-drop-qci2totbyte
- s8-uplnk-drop-qci2totpkt
- s8-uplnk-drop-qci3totbyte
- s8-uplnk-drop-qci3totpkt
- s8-uplnk-drop-qci4totbyte
- s8-uplnk-drop-qci4totpkt
- s8-uplnk-drop-qci5totbyte
- s8-uplnk-drop-qci5totpkt
- s8-uplnk-drop-qci6totbyte
- s8-uplnk-drop-qci6totpkt
- s8-uplnk-drop-qci7totbyte
- s8-uplnk-drop-qci7totpkt
- s8-uplnk-drop-qci8totbyte
- s8-uplnk-drop-qci8totpkt
- s8-uplnk-drop-qci9totbyte
- s8-uplnk-drop-qci9totpkt

- s8-uplnk-drop-othertotbyte
- s8-uplnk-drop-otherpkt
- s8-downlnk-qci1totbyte
- s8-downlnk-qci1totpkt
- s8-downlnk-qci2totbyte
- s8-downlnk-qci2totpkt
- s8-downlnk-qci3totbyte
- s8-downlnk-qci3totpkt
- s8-downlnk-qci4totbyte
- s8-downlnk-qci4totpkt
- s8-downlnk-qci5totbyte
- s8-downlnk-qci5totpkt
- s8-downlnk-qci6totbyte
- s8-downlnk-qci6totpkt
- s8-downlnk-qci7totbyte
- s8-downlnk-qci7totpkt
- s8-downlnk-qci8totbyte
- s8-downlnk-qci8totpkt
- s8-downlnk-qci9totbyte
- s8-downlnk-qci9totpkt
- s8-downlnk-othertotbyte
- s8-downlnk-othertotpkt
- s8-downlnk-drop-qci1totbyte
- s8-downlnk-drop-qci1totpkt
- s8-downlnk-drop-qci2totbyte
- s8-downlnk-drop-qci2totpkt
- s8-downlnk-drop-qci3totbyte
- s8-downlnk-drop-qci3totpkt
- s8-downlnk-drop-qci4totbyte
- s8-downlnk-drop-qci4totpkt
- s8-downlnk-drop-qci5totbyte
- s8-downlnk-drop-qci5totpkt
- s8-downlnk-drop-qci6totbyte
- s8-downlnk-drop-qci6totpkt
- s8-downlnk-drop-qci7totbyte
- s8-downlnk-drop-qci7totpkt
- s8-downlnk-drop-qci8totbyte
- s8-downlnk-drop-qci8totpkt

- s8-downlnk-drop-qci9totbyte
- s8-downlnk-drop-qci9totpkt
- s8-downlnk-drop-othertotbyte
- s8-downlnk-drop-othertotpkt
- s5s8-uplnk-packets
- s5s8-uplnk-bytes
- s5s8-downlnk-packets
- s5s8-downlnk-bytes
- s5s8-uplnk-dropped-packets
- s5s8-uplnk-dropped-bytes
- s5s8-downlnk-dropped-packets
- s5s8-downlnk-dropped-bytes
- s5s8-uplnk-qci1totbyte
- s5s8-uplnk-qci1totpkt
- s5s8-uplnk-qci2totbyte
- s5s8-uplnk-qci2totpkt
- s5s8-uplnk-qci3totbyte
- s5s8-uplnk-qci3totpkt
- s5s8-uplnk-qci4totbyte
- s5s8-uplnk-qci4totpkt
- s5s8-uplnk-qci5totbyte
- s5s8-uplnk-qci5totpkt
- s5s8-uplnk-qci6totbyte
- s5s8-uplnk-qci6totpkt
- s5s8-uplnk-qci7totbyte
- s5s8-uplnk-qci7totpkt
- s5s8-uplnk-qci8totbyte
- s5s8-uplnk-qci8totpkt
- s5s8-uplnk-qci9totbyte
- s5s8-uplnk-qci9totpkt
- s5s8-uplnk-othertotbyte
- s5s8-uplnk-othertotpkt
- s5s8-uplnk-drop-qci1totbyte
- s5s8-uplnk-drop-qci1totpkt
- s5s8-uplnk-drop-qci2totbyte
- s5s8-uplnk-drop-qci2totpkt
- s5s8-uplnk-drop-qci3totbyte
- s5s8-uplnk-drop-qci3totpkt

- s5s8-uplnk-drop-qci4totbyte
- s5s8-uplnk-drop-qci4totpkt
- s5s8-uplnk-drop-qci5totbyte
- s5s8-uplnk-drop-qci5totpkt
- s5s8-uplnk-drop-qci6totbyte
- s5s8-uplnk-drop-qci6totpkt
- s5s8-uplnk-drop-qci7totbyte
- s5s8-uplnk-drop-qci7totpkt
- s5s8-uplnk-drop-qci8totbyte
- s5s8-uplnk-drop-qci8totpkt
- s5s8-uplnk-drop-qci9totbyte
- s5s8-uplnk-drop-qci9totpkt
- s5s8-uplnk-drop-othertotbyte
- s5s8-uplnk-drop-otherpkt
- s5s8-downlnk-qci1totbyte
- s5s8-downlnk-qci1totpkt
- s5s8-downlnk-qci2totbyte
- s5s8-downlnk-qci2totpkt
- s5s8-downlnk-qci3totbyte
- s5s8-downlnk-qci3totpkt
- s5s8-downlnk-qci4totbyte
- s5s8-downlnk-qci4totpkt
- s5s8-downlnk-qci5totbyte
- s5s8-downlnk-qci5totpkt
- s5s8-downlnk-qci6totbyte
- s5s8-downlnk-qci6totpkt
- s5s8-downlnk-qci7totbyte
- s5s8-downlnk-qci7totpkt
- s5s8-downlnk-qci8totbyte
- s5s8-downlnk-qci8totpkt
- s5s8-downlnk-qci9totbyte
- s5s8-downlnk-qci9totpkt
- s5s8-downlnk-othertotbyte
- s5s8-downlnk-othertotpkt
- s5s8-downlnk-drop-qci1totbyte
- s5s8-downlnk-drop-qci1totpkt
- s5s8-downlnk-drop-qci2totbyte
- s5s8-downlnk-drop-qci2totpkt

- s5s8-downlnk-drop-qci3totbyte
- s5s8-downlnk-drop-qci3totpkt
- s5s8-downlnk-drop-qci4totbyte
- s5s8-downlnk-drop-qci4totpkt
- s5s8-downlnk-drop-qci5totbyte
- s5s8-downlnk-drop-qci5totpkt
- s5s8-downlnk-drop-qci6totbyte
- s5s8-downlnk-drop-qci6totpkt
- s5s8-downlnk-drop-qci7totbyte
- s5s8-downlnk-drop-qci7totpkt
- s5s8-downlnk-drop-qci8totbyte
- s5s8-downlnk-drop-qci8totpkt
- s5s8-downlnk-drop-qci9totbyte
- s5s8-downlnk-drop-qci9totpkt
- s5s8-downlnk-drop-othertotbyte
- s5s8-downlnk-drop-othertotpkt

System Schema

- cc-badans-auth-appid
- cc-badans-sessid
- cc-badans-cc-req-num
- cc-badans-cc-req-type
- cc-badans-origin-host
- cc-badans-origin-realm
- cc-badans-parsemsg-err
- cc-badans-parsemscc-err
- cc-badans-misc-err
- dpca-cursess
- dcca-cursess
- asngw-simple-ip-reanchored
- asnpc-cursess
- asnpc-curactive
- asnpc-ttlsetup
- asnpc-retriesexhaust
- asnpc-tidfail
- asnpc-luattempted
- asnpc-ludenied
- asnpc-lucomp
- asnpc-pagattempted

- asnpc-pagsucceeded
- asnpc-annoucetriggered
- phsgw-cursess
- phsgw-cur-active-call
- phsgw-total-sess-setup
- phsgw-retriesexhaust
- phsgw-uplink-sfs
- phsgw-downlink-sfs
- phsgw-tidfail
- phsgw-handoffattempt
- phsgw-handoffdenied
- phsgw-handoffcomp
- phsgw-authsucc
- phsgw-authfailures
- phsgw-3partyauthsucc
- phsgw-3partyauthfailures
- phspc-cursess
- phspc-total-sess-setup
- phspc-retriesexhaust
- phspc-tidfail
- phspc-locupdate-attempt
- phspc-locupdate-denied
- phspc-locupdate-comp
- phspc-paging-attempt
- ikev2-csa-createreqsnt
- ikev2-csa-createreqrcv
- ikev2-csa-createrspsnt
- ikev2-csa-creatersprcv
- ikev2-csa-createsucc
- ikev2-csa-createfail
- ikev2-csa-createsftovrflw
- ikev2-csa-createhrdovrflw
- ikev2-csa-sngldelpldsnt
- ikev2-csa-sngldelpldrcv
- ikev2-csa-multdelpldsnt
- ikev2-csa-multdelpldrcv
- ikev2-csa-delpldsnglspisnt
- ikev2-csa-delpldsnglspircv

- ikev2-csa-delmultspisnt
- ikev2-csa-delmultspisnt
- ikev2-auth-p1finalsent
- ikev2-auth-p1finalrcvd
- ikev2-auth-p2finalsent
- ikev2-auth-p2finalrcvd
- peak-memusage
- uptimestr

Modified Bulk Statistics

The following bulk statistics were modified in Release 11.0.

ECS Schema

- p2p-skype-audio-uplnk-bytes
- p2p-skype-audio-dwlnk-bytes
- p2p-skype-audio-uplnk-pkts
- p2p-skype-audio-dwlnk-pkts
- p2p-skype-non-audio-uplnk-bytes
- p2p-skype-non-audio-dwlnk-bytes
- p2p-skype-non-audio-uplnk-pkts
- p2p-skype-non-audio-dwlnk-pkts
- p2p-msn-audio-uplnk-bytes
- p2p-msn-audio-dwlnk-bytes
- p2p-msn-audio-uplnk-pkts
- p2p-msn-audio-dwlnk-pkts
- p2p-msn-video-uplnk-bytes
- p2p-msn-video-dwlnk-bytes
- p2p-msn-video-uplnk-pkts
- p2p-msn-video-dwlnk-pkts
- p2p-yahoo-audio-uplnk-bytes
- p2p-yahoo-audio-dwlnk-bytes
- p2p-yahoo-audio-uplnk-pkts
- p2p-yahoo-audio-dwlnk-pkts
- p2p-yahoo-non-audio-uplnk-bytes
- p2p-yahoo-non-audio-dwlnk-bytes
- p2p-yahoo-non-audio-uplnk-pkts
- p2p-yahoo-non-audio-dwlnk-pkts
- p2p-oscar-audio-uplnk-bytes

- p2p-oscar-audio-dwlnk-bytes
- p2p-oscar-audio-uplnk-pkts
- p2p-oscar-audio-dwlnk-pkts
- p2p-oscar-non-audio-uplnk-bytes
- p2p-oscar-non-audio-dwlnk-bytes
- p2p-oscar-non-audio-uplnk-pkts
- p2p-oscar-non-audio-dwlnk-pkts
- p2p-gtalk-audio-uplnk-bytes
- p2p-gtalk-audio-dwlnk-bytes
- p2p-gtalk-audio-uplnk-pkts
- p2p-gtalk-audio-dwlnk-pkts
- p2p-gtalk-non-audio-uplnk-bytes
- p2p-gtalk-non-audio-dwlnk-bytes
- p2p-gtalk-non-audio-uplnk-pkts
- p2p-gtalk-non-audio-dwlnk-pkts

LMA Schema

The following statistics were added in this release and replace the associated statistics in parenthises:

- bindupd-denynotlmamobile (bindupd-denynotmobile)

PGW Schema

The following statistics were added in this release and replace the associated statistics in parenthises:

- handoverstat-intersgsnatt (handoverstat-ersgsnatt)
- handoverstat-intersgsnsucc (handoverstat-ersgsnsucc)
- handoverstat-intersgsnfail (handoverstat-ersgsnfail)
- handoverstat-intersgwatt (handoverstat-ersgwatt)
- handoverstat-intersgwsucc (handoverstat-ersgwsucc)
- handoverstat-intersgwfail (handoverstat-ersgwfail)
- handoverstat-interhsgwsucc (handoverstat-erhsgwsucc)
- handoverstat-interhsgwsucc (handoverstat-erhsgwsucc)
- handoverstat-interhsgwfail (handoverstat-erhsgwfail)

S-GW Schema

The following statistics were added in this release and replace the associated statistics in parenthises:

- intersgwhaovstat-pdnin-x2 (interhaovstat-pdnin-x2)
- intersgwhaovstat-pdnin-idletau (interhaovstat-pdnin-idletau)
- intersgwhaovstat-pdnin-s1 (interhaovstat-pdnin-s1)
- intersgwhaovstat-pdnout (interhaovstat-pdnout)

- intrasgwhaovstat-intramme (interhaovstat-intra-intramme)
- intrasgwhaovstat-intermme (interhaovstat-intra-intermme)

Obsoleted Bulk Statistics

The following bulk statistics were obsoleted in Release 11.0.

GTP-C Schema

- dyn_ppp_attempt
- dyn_ppp_success

IMSA Schema

- dpca-sessfail

MME Schema

- mme-attached-current
- mme-idle-current
- mme-connected-current
- mme–attach–total
- mme–attach–success
- mme–attach–failure
- mme–auth–total
- mme–auth–success
- mme–auth–failure
- mme–identity–total
- mme–identity–success
- mme–identity–failure
- mme–security–total
- mme–security–success
- mme–security–failure
- mme–handover_x2–total
- mme–handover_x2 success
- mme–handoveR_x2–failure
- mme–handoveR_s1–total
- mme–handover_s1–success
- mme–handover_s1–failure
- mme–tau–total
- mme–tau–success
- mme-tau-failure
- mme-detach-total
- mme-detach-success

- mme-detach-failure
- mme-idle_mode_entry-total
- mme-idle_mode_entry-success
- mme-idle_mode_entry-failure
- mme-service_req-total
- mme–service_req-success
- mme-service_req-failure
- mme-paging-total
- mme-paging-success
- mme-paging-failure
- mme-pdn_connect-total
- mme-pdn_connect-success
- mme-pdn_connect-failure
- mme-pdn_disconnect-total
- mme-pdn_disconnect-success
- mme-pdn_disconnect-failure
- mme-dflt_brr_activation-total
- mme-dflt_brr_activation-success
- mme-dflt_brr_activation-failure
- mme–dedi_brr_activation-total
- mme–dedi_brr_activation-success
- mme–dedi_brr_activation-failure
- mme-brr_deactivation–total
- mme-brr_deactivation-success
- mme-brr_deactivation-failure
- mme-rx_emm-total
- mme-rx_emm-plain_nas
- mme-rx_emm-integrity
- mme-rx_emm-ciphered
- mme-rx_emm-parsing_failed
- mme-rx_emm-accepted
- mme-rx_emm-ignored
- mme-rx_emm-denied
- mme-rx_esm-total
- mme-rx_esm-plain_nas
- mme-rx_esm-integrity
- mme-rx_esm-ciphered
- mme-rx_esm-parsing_failed

- mme-rx_esm-accepted
- mme-rx_esm-ignored
- mme-rx_esm-denied
- mme-tx_emm-total
- mme-tx_emm-plain_nas
- mme-tx_emm-integrity
- mme-tx_emm-ciphered
- mme-tx_emm- lower_layer_failure
- mme-tx_emm- retransmitted
- mme-tx_esm-total
- mme-tx_esm-plain_nas
- mme-tx_esm-integrity
- mme-tx_esm-ciphered
- mme-tx_esm- lower_layer_failure
- mme-tx_esm- retransmitted
- vsncp-fail-unk

PPP Schema

- auth-attempt-ppp

SGSN Schema

- ps-inter-service-rau-rej-total
- intra-sgsn-inter-system-gsm-to-wcdma-success
- intra-sgsn-inter-system-gsm-to-wcdma-rej
- intra-sgsn-inter-system-gsm-to-wcdma-fail
- intra-sgsn-inter-system-wcdma-to-gsm-success
- intra-sgsn-inter-system-wcdma-to-gsm-rej
- intra-sgsn-inter-system-wcdma-to-gsm-fail
- inter-system-2G-to-3G-rau-requests
- inter-system-2G-to-3G-rau-accepts
- inter-system-2G-to-3G-rau-rejects
- inter-system-2G-to-3G-comb-rau-requests
- inter-system-2G-to-3G-comb-rau-accepts
- inter-system-2G-to-3G-comb-rau-rejects
- inter-system-3G-to-2G-rau-requests
- inter-system-3G-to-2G-rau-accepts
- inter-system-3G-to-2G-rau-rejects
- inter-system-3G-to-2G-comb-rau-requests
- inter-system-3G-to-2G-comb-rau-accepts

- inter-system-3G-to-2G-comb-rau-rejects
- ps-inter-rat-rau-total
- comb-inter-rat-rau-total
- ret-ps-inter-rat-rau-total
- ret-comb-inter-rat-rau-total
- ps-inter-service-rau-total
- comb-inter-service-rau-total
- ret-ps-inter-service-rau-total
- ret-comb-inter-service-rau-total
- ps-inter-rat-rau-acc-total
- comb-inter-rat-rau-acc-total
- ret-ps-inter-rat-rau-acc-total
- ret-comb-inter-rat-rau-acc-total
- ps-inter-service-rau-acc-total
- comb-inter-service-rau-acc-total
- ret-ps-inter-service-rau-acc-total
- ret-comb-inter-service-rau-acc-total
- ps-inter-rat-rau-rej-total
- comb-inter-rat-rau-rej-total
- comb-inter-service-rau-rej-total
- 3G-cs-page-response
- 2G-cs-page-response

System Schema

- asngw-cursess
- asngw-curactive
- asngw-ttlsetup
- asngw-retriesexhaust
- asngw-sfs
- asngw-tidfail
- asngw-handoffattempt
- asngw-handoffdenied
- asngw-handoffcomp
- asngw-authsucc
- asngw-authfailures
- asngw-cur-active-call
- asngw-total-sess-setup
- asngw-retriesexhaust
- asngw-sfs

- asngw-tidfail
- asngw-handoffattempt
- asngw-handoffdenied
- asngw-handoffcomp
- asngw-authsucc
- asngw-authfailures
- cf-dyn-rateblock
- cf-cat-adv-pkts-hit
- cf-cat-adv-pkts-block
- cf-cat-auct-pkts-hit
- cf-cat-auct-pkts-block
- cf-cat-clean-pkts-hit
- cf-cat-clean-pkts-block
- cf-cat-cporn-pkts-hit
- cf-cat-cporn-pkts-block
- cf-cat-esrb-pkts-hit
- cf-cat-esrb-pkts-block
- cf-cat-p2p-pkts-hit
- cf-cat-p2p-pkts-block
- cf-cat-phish-pkts-hit
- cf-cat-phish-pkts-block
- cf-cat-radio-pkts-hit
- cf-cat-radio-pkts-block
- cf-cat-sftwre-pkts-hit
- cf-cat-sftwre-pkts-block
- cf-cat-spywre-pkts-hit
- cf-cat-spywre-pkts-block
- cf-cat-susp-pkts-hit
- cf-cat-susp-pkts-block
- ikev2-notifpaysent-noaddsa
- ikev2-notifpayrecv-noaddsa
- swbuild

Web Element Manager Path

Click Accounting | Bulk Statistics Configuration.

RADIUS Attributes in Release 11.0

This section lists additions and changes to RADIUS AVPs in Release 11.0. Refer to the *AAA Interface Configuration and Reference* for details.

New Attributes

The following RADIUS attributes are new in Release 11.0.

- 3GPP2-FEID
- 3GPP2-IP-Services-Authorized
- 3GPP2-PMIP-Capability
- 3GPP2-PMIP-IPv4Session-Info
- 3GPP2-PMIP-IPv6Session-Info
- 3GPP2-PMIP-NAI
- 3GPP-Allocate-IPType
- 3GPP-GGSN-IPv6-Address
- 3GPP-IPv6-DNS-Servers
- 3GPP-SGSN-IPv6-Address
- Geographical-Location
- HNB-Internet-Information
- HNB-Parameters
- Macro-Coverage-Information
- Reject-Cause
- SN-DHCP-Options
- SN-Proxy-MIPV6
- SN-TPO-Policy
- White-List

Modified Attributes

The following RADIUS attributes were modified in Release 11.0.

- 3GPP2-IP-QOS
- 3GPP-Negotiated-QOS-Profile
- 3GPP-User-Location-Info
- Hotline-Indicator
- Hotline-Profile-ID
- Hotlining-Capabilities
- PMIP-Authenticated-Nwk-Id
- SN1-Disconnect-Reason
- SN1-GTP-Version

- SN1-QoS-Negotiated
- SN1-QoS-Traffic-Policy
- SN1-Service-Type
- SN-Disconnect-Reason
- SN-GTP-Version
- SN-QoS-Negotiated
- SN-QoS-Traffic-Policy
- SN-Service-Type

Removed Attributes

The following RADIUS attributes were removed in Release 11.0.

None for this release.

Diameter Attributes in Release 11.0

This section lists additions and changes to Diameter attributes in Release 11.0. Refer to the *AAA Interface Reference* for details.

New Attributes

The following Diameter attributes are new in Release 11.0.

- Accounting-PCC-R3-P-Capability
- Anchor-Data-Path-Address
- Max-Requested-Bandwidth
- Packet-Data-Flow-Info
- Packet-Interval
- Packet-Size
- PDFID
- Routing-Policy
- Send-Data-Indication
- Session-Linking-Indicator
- SN-Fast-Reauth-Username
- SN-Pseudonym-Username
- Starent-Subscriber-Permission
- Subs-Req-Type
- WiMAX-A-PCEF-Address
- WiMAX-PCC-R3-P-Capability
- WiMAX-QoS-Information
- WiMAX-Release
- WLAN-Session-Id

Modified Attributes

The following Diameter attributes were modified in Release 11.0.

- 3GPP-Trigger-Type
- ANID
- Event-Report-Indication
- Experimental-Result-Code
- IP-CAN-Type
- PDG-CHARGING-ID
- Trace-Depth

Removed Attributes

The following Diameter attributes were removed in Release 11.0.

None for this release.

Web Element Manager Enhancements

Support for Viewing SSC Alarm and Bulkstat Information

WEM now supports the viewing of alarm and bulkstat information for a specified Cisco Subscriber Service Controller (SSC). Users can add one or more SSCs to WEM via the NE (Network Element) List dialog box. Once the SSCs have been added, users will be able to select the SSC for viewing a variety of Alarm and Bulkstat information via the Alarm Management and Accounting menus.

IMPORTANT

Alarm and bulkstat configuration first must be performed via the SSC's Command Line Interface before that information will be available for viewing in WEM.

Web Element Manager Path:

- Accounting\Bulk Statistics Configuration
- Alarm Management\Current Alarm View
- Alarm Management\Historical Alarm View
- Alarm Management\Pending Alarm View

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 11.0. New commands in this version are divided into the following sections:

Common Commands - New in Release 11.0

None for this release.

Content Filtering Commands - New in Release 11.0

None for this release.

ECS Commands - New in Release 11.0

None for this release.

Firewall Commands - New in Release 11.0

The following Stateful Firewall commands are new in Release 11.0.

show active-charging flow-mappings all

A new command displaying the flow-mappings statistics/counters was added in this release.

CLI (Exec Mode)

show active-charging flow-mappings [all | call-id *callid* **| [nat { not-required | required [nat-realm** *realm_name* **] } | trans-proto { tcp | udp }] + [| { grep** *grep_options* **| more }]**

Web Element Manager Path

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

GGSN Commands - New in Release 11.0

The following GGSN commands are new in Release 11.0.

show apn statistics name

Following new counters added under “Data Statistics” section:

- uplink Flow MBR excd byte drop
- downlink Flow MBR excd byte drop
- uplink Flow MBR excd packet drop
- downlink Flow MBR excd packet drop
- uplink Flow GBR excd byte drop
- downlink Flow GBR excd byte drop
- uplink Flow GBR excd packet drop
- downlink Flow GBR excd packet drop
- uplink AMBR excd byte drop
- downlink AMBR excd byte drop
- uplink AMBR excd packet drop
- downlink AMBR excd packet drop
- uplink misc byte drop
- downlink misc byte drop
- uplink misc packet drop
- downlink misc packet drop

Web Element Manager Path

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

HA Commands - New in Release 11.0

None for this release.

MME Commands - New in Release 11.0

The following MME commands are new in Release 11.0.

clear hss-peer-service

Clears statistic information for HSS peer services configured on the system.

CLI (Exec Mode)

clear hss-peer-service [statistics [service *name* **]**

Web Element Manager Path

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

clear sgs-service

Clears SGs service statistics for all SGs services, known Visitor Location Registers (VLRs), or a specific SGs service or VLR name.

CLI (Exec Mode)

clear sgs-service { statistics [name *name* **] | vlr-status [service-name** *name* **] [vlr-name** *name* **] }**

Web Element Manager Path

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

show hss-peer-service

A new command displaying information about configured HSS peer services on the system is included in this release.

CLI (Exec Mode)

show hss-peer-service { service { all | name *name* **} | session { all | callid** *id* **| full | mdn** *mdn* **| nai** *nai* **| summary } | statistics { all | service** *name* **| summary } }**

Web Element Manager Path

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

show mme-policy

Displays information for MME policy configurations on this system including handover restriction lists, subscriber maps, and tracking area identifiers (TAIs).

CLI (Exec Mode)

show mme-policy { ho-restriction-list { name *name* **| summary } | subscriber-map { name** *name* **| summary } | tai-mgmt-db { name** *name* **| summary } } [| { grep** *grep_options* **| more }]**

Web Element Manager Path

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

show sgs-service

A new command displaying information about configured SGs services on the system is included in this release.

CLI (Exec Mode)

```
show sgs-service { all | name name | statistics { all | name name } |
vlr-status [ service-name name ] [ vlr-name name ] [ full ]
```

Web Element Manager Path

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

NAT Commands - New in Release 11.0

The following NAT commands are new in Release 11.0.

show active-charging flow-mappings all

A new command displaying information for all the active charging flow-mappings based on applied filters was added in this release.

CLI (Exec Mode)

```
show active-charging flow-mappings [ all | call-id callid | [ nat {
not-required | required [ nat-realm realm_name ] } | trans-proto { tcp |
udp } ] + [ | { grep grep_options | more } ]
```

Web Element Manager Path

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

PDIF Commands - New in Release 11.0

None for this release.

PDSN Commands - New in Release 11.0

None for this release.

Peer-to-Peer - New in Release 11.0

None for this release.

SGSN Commands - New in Release 11.0

None for this release.

Serving Gateway Commands - New in Release 11.0

The following Serving Gateway (S-GW) commands are new in Release 11.0.

show ca-crl

A new command displaying information for Certificate Authority (CA) Certificate Revocation List (CRL) is included in this release.

CLI (Exec Mode)

show ca-crl (all | name *name* **}**

Web Element Manager Path

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

Modified Commands

This section contains performance management commands that have been modified in Release 11.0. Modified commands in this version are divided into the following sections:

- *Common Commands - Modified in Release 11.0*
- *Content Filtering Commands - Modified in Release 11.0*
- *ECS Commands - Modified in Release 11.0*
- *Firewall Commands - Modified in Release 11.0*
- *GGSN Commands - Modified in Release 11.0*
- *HA Commands - Modified in Release 11.0*
- *NAT Commands - Modified in Release 11.0*
- *PDIF Commands - Modified in Release 11.0*
- *PDSN Commands - Modified in Release 11.0*
- *Peer-to-Peer Commands - Modified in Release 11.0*
- *Serving Gateway Commands - Modified in Release 11.0*
- *Session Control Manager Commands - Modified in Release 11.0*
- *SGSN Commands - Modified in Release 11.0*

Common Commands - Modified in Release 11.0

The following common commands have been modified in Release 11.0.

logging filter active facility

This command configures logging filter settings for specified facilities. This command now supports the keyword **`diameter-dns`**, which enables the new logging facility diameter-dns.

CLI (Exec Mode)

`logging filter active facility diameter-dns level` *`severity_level`* **`[ critical-info | no-critical-info ]`**

Web Element Manager Path

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

show aaa group name default

This command displays AAA statistics for the current context. The output of this command includes the following new fields:

- serving-node change trigger
- rat-change trigger
- uli-change trigger
- rai-change trigger
- qos-change trigger
- ms-timezone-change trigger

CLI (Exec Mode)

`show aaa { group { all | name` *`aaa_group_name`* **`} | local counters } [ | { grep`** *`grep_options`* **`| more } ]`**

Web Element Manager Path

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

show apn all

This command has been enhanced to display all the configured GTPP groups and the corresponding accounting contexts in the APN.

CLI (Exec Mode)

`show apn all`

Web Element Manager Path

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

show configuration verbose

This command displays current configuration information. When RADIUS triggers are configured, the output of this command includes the following new fields:

- radius trigger qos-change

- radius trigger serving-node-change
- radius trigger uli-change
- radius trigger rat-change
- radius trigger rai-change
- radius trigger ms-timezone-change

CLI (Exec Mode)

`show configuration verbose`

Web Element Manager Path

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

show diameter statistics

This command displays Diameter peer statistics. The output of the "**`show diameter statistics`**" and "**`show diameter statistics proxy`**" commands include the following new fields:

- Diameter DNS Statistics:
  - DNS Init
  - DNS De-Init
  - VPN Init Request
  - VPN Init Response
  - VPN Init Success
  - VPN Init Timeout
  - DNS A Requests
  - DNS A Responses
  - DNS A Hits
  - DNS A Timeouts
  - DNS AAAA Requests
  - DNS AAAA Responses
  - DNS AAAA Hits
  - DNS AAAA Timeouts
  - DNS NAPTR Requests
  - DNS NAPTR Responses
  - DNS NAPTR Hits
  - DNS NAPTR Timeouts
  - DNS SRV Requests
  - DNS SRV Responses
  - DNS SRV Hits
  - DNS SRV Timeouts
  - A Type App Request
  - AAAA Type App Request

- NAPTR Type App Request

CLI (Exec Mode)

show diameter statistics [[proxy] endpoint *endpoint_name* **[peer-host** *peer_id* **[peer-realm** *realm_id* **]]] [| { grep** *grep_options* **| more }]**

Web Element Manager Path

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

show dynamic-policy statistics

This command displays policy control and charging (PCC) statistics from the interface communicating with the PCRF (Gx(x)). A new field “UE Time Zone change” has been added to the output of this command.

CLI (Exec Mode)

show dynamic-policy statistics { hsgw-service *name* **| pdsn-service** *name* **| sgw-service** *name* **}**

Web Element Manager Path

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

show ims-authorization service statistics

This command displays statistics of all/specific IP Multimedia Subsystem (IMS) authorization service. The output of this command includes the following field:

Usage Volume Threshold

CLI (Exec Mode)

show ims-authorization service statistics

Web Element Manager Path

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

show ims-authorization sessions full

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:

Event Report Indication

CLI (Exec Mode)

show ims-authorization session [full | summary] | [all | [ims-auth-service *ims_auth_svc_name* **| imsi** *imsi_value* **[nsapi** *nsapi_value* **] | apn** *apn_name* **| ip-address** *ip_address* **| callid** *call_id* **] [| { 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 fields:

- Session ID
- UE IP Address
  - UE IP Session Type
  - IPv4 Address
  - IPv6 Address
- Primary OCS
- Secondary OCS
- Primary CCF
- Secondary CCF

CLI (Exec Mode)

show ims-authorization session [full | summary] | [all | [ims-auth-service *ims_auth_svc_name* **| imsi** *imsi_value* **[nsapi** *nsapi_value* **] | apn** *apn_name* **| ip-address** *ip_address* **| callid** *call_id* **] [| { grep** *grep_options* **| more }]**

Web Element Manager Path

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

show radius accounting servers detail

The output of this command includes the following new field:

Keepalive Representative Group

CLI (Exec Mode)

show radius accounting servers [admin-status | detail | radius]

Web Element Manager Path

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

show radius authentication servers detail

The output of this command includes the following new field:

Keepalive Representative Group

CLI (Exec Mode)

show radius authentication servers [admin-status | detail | radius]

Web Element Manager Path

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

show srp checkpoint statistics

This command displays Service Redundancy Protocol information.

The output of this command includes the following new fields:

- total acs-sess-info micro-chkpnt rcvd
- total acs-sess-info micro-chkpnt sent

CLI (Exec Mode)

show srp checkpoint statistics [| { grep *grep_options* **| more }]**

Web Element Manager Path

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

show subscribers cscf-only full

This command displays per-subscriber information for active sessions.

The output of this command includes the following new fields:

- DIAMETER Policy Session-Id
- DIAMETER Policy Subscription

CLI (Exec Mode)

show subscribers cscf-only full

Web Element Manager Path

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

show subscribers full

This command has been enhanced to display the following fields:

- GTPP Group
- Acct Context

CLI (Exec Mode)

show subscribers full

Web Element Manager Path

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

show subscribers policy

This command displays information for subscriber sessions defined by the specified keywords. A new field “UE Time Zone change” has been added to the output of this command.

CLI (Exec Mode)

show subscribers policy

Web Element Manager Path

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

Content Filtering Commands - Modified in Release 11.0

None for this release.

ECS Commands - Modified in Release 11.0

The following ECS commands have been modified in Release 11.0.

clear active-charging tcp-proxy statistics

This command clears TCP Proxy statistics. The following keywords were added to this command:

- **all**
- **ip-layer**
- **tcp-layer**

CLI (Exec Mode)

clear active-charging tcp-proxy statistics [all | ip-layer | rulebase *rulebase_name* **| tcp-layer]**

Web Element Manager Path

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

show active-charging credit-control statistics

This command displays statistics for Diameter/RADIUS prepaid credit control service in the Active Charging Service.

The counter header “Bad Answer Stats” has been renamed to “CC Bad Answer Stats”.

CLI (Exec Mode)

show active-charging credit-control { statistics [all | group *group_name* **] | session-states [rulebase** *rulebase_name* **] [content-id** *content_id* **] } [| { grep** *grep_options* **| more }]**

Web Element Manager Path

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

show active-charging edr-udr-file statistics

The output of this command includes the following new field:

- Overall Statistics:
  - Num of times PUSH cancelled due to HD failure: The number of times EDR/UDR push was cancelled due to hard disk failures.

CLI (Exec Mode)

show active-charging edr-udr-file 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 rulebase statistics

This command displays active charging rulebase statistics. The output of this command includes the following new field:

TCP-proxy reset for non-SYN flows: The number of resets sent by proxy for flows with no SYN packet after recovery

CLI (Exec Mode)

show active-charging rulebase statistics [name *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 all available information for all active charging sessions. The output of this command includes the following new fields:

- Bearer BW Limit Upl Pkts
- Bearer BW Limit Dnl Pkts
- Bearer BW Limit Upl Bytes
- Bearer BW Limit Dnl Bytes
- PCC Rule BW Limit Upl Pkts
- PCC Rule BW Limit Dnl Pkts
- PCC Rule BW Limit Upl Bytes
- PCC Rule BW Limit Dnl Bytes
- PCC Rule Gating Upl Pkts
- PCC Rule Gating Dnl Pkts
- PCC Rule Gating Upl Bytes
- PCC Rule Gating Dnl Bytes

CLI (Exec Mode)

show active-charging sessions full [| { 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 all

This command displays all available information for all active charging sessions. The output of this command includes the following new fields:

- CC Group: The credit control group selected.
- Current TCP Proxy Flows: The number of current TCP Proxy flows

- Total TCP Proxy Flows: The total number of TCP Proxy flows for the session
- TCP-proxy reset for non-SYN flows: The number of resets sent by TCP Proxy for flows with no SYN packet after recovery

In addition, in this release the “Trigger-Type” AVP supports the value CHANGE_IN_SERVING_NODE (61). When used, it can be verified in the output of this command in the Pending Triggers field.

CLI (Exec Mode)

`show active-charging sessions full all [ | { grep` *`grep_options`* **`| more } ]`**

Web Element Manager Path

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

show active-charging tcp-proxy statistics

This command displays TCP Proxy statistics. The following keywords were added to this command:

- **`all`**
- **`ip-layer`**
- **`tcp-layer`**

CLI (Exec Mode)

`show active-charging tcp-proxy statistics [ all | ip-layer | rulebase` *`rulebase_name`* **`| tcp-layer ] [ 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 tcp-proxy statistics

This command displays TCP Proxy statistics.

With the **`all`** and **`tcp-layer`** options the output of this command includes the following new fields:

- Incoming TCP Bytes
- In TCP Retrans Seg
- In TCP Retrans Byte

New fields shown with optional **`verbose`** keyword:

- In TCP Partial Retr Seg
- In TCP Partial Retr Byte
- In TCP OOO Segments
- In TCP OOO Bytes
- In TCP OOO+Retrans Seg
- In TCP OOO+Retrans Bytes

- In TCP OOO Succ Seg
- In TCP OOO Succ Bytes
- In TCP Csum Err Seg
- In TCP Csum Err Bytes

New fields shown in the output for **`show active-charging tcp-proxy statistics all verbose`** command:

- Proxy Session counters:
  - Current Connecting Conn (AO on GN)
  - Current Connecting Conn (AO on GI)
  - Current Connected Conn (AO on GN)
  - Current Connected Conn (AO on GI)
  - Current Un-Accepted Conn (PO on GN)
  - Current Un-Accepted Conn (PO on GI)
  - Current Accepted Conn (PO on GN)
  - Current Accepted Conn (PO on GI)
  - Current EST conn on both side
  - Total PO Succ on GN
  - Total AO Succ on GI
  - Total PO Succ on GI
  - Total AO Succ on GN
  - Flows not proxied - Proxy flow limit
  - Flows not proxied - Backlog limit
  - Flows not proxied - Gn sock limit
  - Flows not proxied - Gi sock limit
  - Flows cleared - incomplete active open
  - Flows cleared - incomplete passive open
- Proxy Error counters
- Socket Open Failed on Gn:
  - No Errors
  - No Permission
  - No Memory
  - Invalid Arg
  - Too Many Sockets
  - Others
- Socket Open Failed on Gi
  - No Errors
  - No Permission
  - No Memory

  - Invalid Arg
  - Too Many Sockets
  - Others
- Socket Error Events on Gn
  - No Errors
  - No Permission
  - No Memory
  - No Access
  - Operation Would Block
  - Operation in Progress
  - Connection Reset by Peer
  - Send After Shutdown
  - Operation Timedout
  - Connection Refused
  - Too Many Sockets
  - Others
- Socket Error Events on Gi
  - No Errors
  - No Permission
  - No Memory
  - No Access
  - Operation Would Block
  - Operation in Progress
  - Connection Reset by Peer
  - Send After Shutdown
  - Operation Timedout
  - Connection Refused
  - Too Many Sockets
  - Others

CLI (Exec Mode)

`show active-charging tcp-proxy statistics [ all | tcp-layer ] [ verbose ] [ | { grep` *`grep_options`* **`| more } ]`**

Web Element Manager Path

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

Firewall Commands - Modified in Release 11.0

The following Stateful Firewall commands have been modified in Release 11.0.

show active-charging analyzer statistics name sip

This command displays active charging protocol analyzer statistics for the SIP analyzer. The following new fields are added to the output of this command to display SIP traffic statistics that are captured by the SIP Analyzer:

- SIP Advanced Session Stats
  - Total Uplink Bytes
  - Total Downlink Bytes
  - Total Uplink Packets
  - Total Downlink Packets
  - SIP Calls
- SIP Request
- Total Received
- Total Transmitted
- Retransmitted
- SIP Response
- Total Received
- Total Transmitted
- Retransmitted

CLI (Exec Mode)

show active-charging analyzer statistics name sip [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 Firewall-and-NAT Policy information. The following fields were added to the output of this command: The new field “Action upon receiving an ICMP echo packet with id zero” is added to the output of this command to allow/deny the echo packets with ICMP ID zero.

- Action upon receiving an ICMP echo packet with id zero
- TCP Partial Connection Timeout

CLI (Exec Mode)

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

Web Element Manager Path

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

show active-charging subsystem

This command displays active charging subsystem information. The keyword **sip** was added to this command.

CLI (Exec Mode)

show active-charging subsystem { all | facility acsmgr { all | instance *instance_value* **} [rulebase name** *rulebase_name* **] | sip } [| { 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 to display the total and current Firewall/NAT enabled calls:

- Firewall/NAT Subscribers:
  - Firewall Enabled
  - NAT enabled
  - Firewall and NAT enabled

CLI (Exec Mode)

show active-charging subsystem { all | facility acsmgr { all | instance *instance_value* **} [rulebase name** *rulebase_name* **] | sip } [| { 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 11.0

The following GGSN commands have been modified in Release 11.0.

show apn all

The statistics under “3gpp qos to dscp mapping” modified to the following list of counters:

- qci 1: ef
- qci 2: ef
- qci 3: af11
- qci 4: af11
- qci 5: ef
- qci 6: ef
- qci 7: af21
- qci 8: af21
- qci 9: be

The statistics under “3gpp qos to dscp mapping based on Alloc, Prio” modified to the following list of counters:

- qci 5 (Alloc.P 1): ef
- qci 5 (Alloc.P 2): ef
- qci 5 (Alloc.P 3): ef
- qci 6 (Alloc.P 1): ef
- qci 6 (Alloc.P 2): ef
- qci 6 (Alloc.P 3): ef
- qci 7 (Alloc.P 1): af21
- qci 7 (Alloc.P 2): af21
- qci 7 (Alloc.P 3): af21
- qci 8 (Alloc.P 1): af21
- qci 8 (Alloc.P 2): af21
- qci 8 (Alloc.P 3): af21

show apn statistics name

Due to support for both IPv4 and IPv6 IP types, the following modified counters under “Data Statistics” section as:

- ip bad hdr
- ip ttl exceeded
- ip fragments sent
- ip could not fragment
- ip input acl drop
- ip output acl drop
- ip input css down drop

- ip output css down drop
- ip early pdu rcvd
- IP bad length trim
- ip source violations
- ip source violations no accounting
- ip source violation ignored

CLI (Exec Mode)

show apn all

Web Element Manager Path

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

show gtpc statistics

Option ‘apn-name’ modified to ‘apn’. Additionally following new options included in this command:

- **gtpcmgr-instance**: Retrieves information from a particular GTPCMgr Instance. gtpcmgr_value can be an integer value from 1 to 4294967295.
- **smgr-instance**: Retrieves information from particular Sessmgr Instance. smgr_value can be an integer value from 1 to 4294967295.
- **format1**: Specifies that more detailed statistics breakup will be displayed.

CLI (Exec Mode)

show gtpc statistics [apn *apn_name* **| ggsn-service** *svc_name* **| sgsn-address** *IPv4_addr* **] [format1 | verbose] | [custom1 | custom2 | gtpcmgr-instance** *gtpcmgr_value* **| smgr-instance** *smgr_value* **] [apn | format1 | ggsn-service | sgsn-address | verbose] | [verbose] [format] | format1**

Web Element Manager Path

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

show gtpc statistics verbose

QoS Traffic classes modified from classes Conversational, Streaming, Interactive 1 through 3, and Background to QCI 1 .... QCI 9. The following counters were modified to the output of this command:

QoS QCI Stats

- QCI 1
  - CPC QoS Accepted
  - CPC QoS Downgraded
  - UPC QoS Accepted
  - UPC QoS Downgraded
- QCI 2
  - CPC QoS Accepted

    - CPC QoS Downgraded
    - UPC QoS Accepted
    - UPC QoS Downgraded
- QCI 3
    - CPC QoS Accepted
    - CPC QoS Downgraded
    - UPC QoS Accepted
    - UPC QoS Downgraded
- QCI 4
    - CPC QoS Accepted
    - CPC QoS Downgraded
    - UPC QoS Accepted
    - UPC QoS Downgraded
- QCI 5
    - CPC QoS Accepted
    - CPC QoS Downgraded
    - UPC QoS Accepted
    - UPC QoS Downgraded
- QCI 6
    - CPC QoS Accepted
    - CPC QoS Downgraded
    - UPC QoS Accepted
    - UPC QoS Downgraded
- QCI 7
    - CPC QoS Accepted
    - CPC QoS Downgraded
    - UPC QoS Accepted
    - UPC QoS Downgraded
- QCI 8
    - CPC QoS Accepted
    - CPC QoS Downgraded
    - UPC QoS Accepted
    - UPC QoS Downgraded
- QCI 9
    - CPC QoS Accepted
    - CPC QoS Downgraded
    - UPC QoS Accepted
    - UPC QoS Downgraded

CLI (Exec Mode)

show gtpc statistics verbose [format1]

Web Element Manager Path

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

HA Commands - Modified in Release 11.0

None for this release.

NAT Commands - Modified in Release 11.0

The following NAT commands have been modified in Release 11.0.

show active-charging analyzer statistics name sip

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

- SIP Advanced Session Stats
  - Total Uplink Bytes
  - Total Downlink Bytes
  - Total Uplink Packets
  - Total Downlink Packets
  - SIP Calls
- SIP Request
- Total Received
- Total Transmitted
- Retransmitted
- SIP Response
- Total Received
- Total Transmitted
- Retransmitted

CLI (Exec Mode)

show active-charging analyzer statistics name sip [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

This command displays active charging subsystem information. The following changes were made to this command:

- The keyword **sip** was added to this command.
- The following fields were removed from the output of **show active-charging subsystem all** command:
  - Total Firewall Subscribers
  - Total NAT Subscribers

CLI (Exec Mode)

show active-charging subsystem { all | facility acsmgr { all | instance *instance_value* **} [rulebase name** *rulebase_name* **] | sip } [| { 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 to display the total and current Firewall/NAT enabled calls:

- Firewall/NAT Subscribers:
  - Firewall Enabled
  - NAT enabled
  - Firewall and NAT enabled

CLI (Exec Mode)

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

Web Element Manager Path

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

show active-charging charging-action name

This command displays information for charging actions configured in the ACS service. The output of this command includes the following new field to display the configured flow-mapping timeout value:

Flow-Mapping Idle Timeout

CLI (Exec Mode)

show active-charging charging-action { { { all | name *charging_action_name* **} [service name** *acs_service_name* **] } | statistics [name** *charging_action_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 service name

This command displays the ACS service details. The output of this command includes the following new fields to display the configured flow-mapping timeout values:

- TCP Flow-Mapping Idle Timeout
- UDP Flow-Mapping Idle Timeout

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 fw-and-nat policy name

This command displays Firewall-and-NAT Policy information. The following new fields are added to the output of this command:

- Uplink NAT-Realm
- Uplink Fw-and-nat-action
- Downlink NAT-Realm
- Downlink Fw-and-nat-action
- Default NAT-Realm
- Default Fw-and-nat-action

CLI (Exec Mode)

show active-charging subsystem { all | facility acsmgr { all | instance *instance_value* **} [rulebase name** *rulebase_name* **] | sip } [| { 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 11.0

None for this release.

PDSN Commands - Modified in Release 11.0

None for this release.

Peer-to-Peer Commands - Modified in Release 11.0

The following Peer-to-Peer commands have been modified in Release 11.0.

clear active-charging analyzer statistics

This command supports the clearing of protocol analyzer statistics for the following P2P applications:

- Armagettron
- Blackberry
- Citrix
- Clubpenguin
- Crossfire
- Dofus
- Facebook
- Fiesta
- Florensia
- Funshion
- Guildwars
- Icecast
- ISAKMP
- Kontiki
- Maplestory
- Meebo
- MGCP
- Octoshape
- OFF
- PS3
- Real Media Stream
- Rfactor
- Shoutcast
- Splashfighter
- SSDP
- StealthNet

- STUN
- TeamSpeak
- Thunder
- Tor
- Truphone
- Veoh TV
- WII
- Windows Media Stream
- World of Kungfu
- XDCC
- YourFreedom

CLI (Exec Mode)

`clear active-charging charging-action statistics [ name` *string* **`] [ | { 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

This command displays the information for the active charging flows. The P2P protocol type flows now support the following applications:

- Armagettron
- Blackberry
- Citrix
- Clubpenguin
- Crossfire
- Dofus
- Facebook
- Fiesta
- Florensia
- Funshion
- Guildwars
- Icecast
- ISAKMP
- Kontiki
- Maplestory
- Meebo
- MGCP
- Octoshape
- OFF

- PS3
- Real Media Stream
- Rfactor
- Shoutcast
- Splashfighter
- SSDP
- StealthNet
- STUN
- TeamSpeak
- Thunder
- Tor
- Truphone
- Veoh TV
- WII
- Windows Media Stream
- World of Kungfu
- XDCC
- YourFreedom

CLI (Exec Mode)

show active-charging flows { all | [connected-time [< | > | greater-than | less-than] *seconds* **] [flow-id** *flow_id* **] [full] [idle-time [< | > | greater-than | less-than]** *seconds* **] [ip-address [server | subscriber] [< | > | IPv4 | greater-than | less-than]** *address* **] [nat { not-required | required [nat-ip** *nat_ip_address* **] }] [port-number [server | subscriber] [< | > | IPv4 | greater-than | less-than]** *number* **] [rx-bytes [< | > | greater-than | less-than]** *number* **] [rx-packets [< | > | greater-than | less-than]** *number* **] [session-id** *session_id* **] [summary] [trans-proto { icmp | tcp | udp }] [tx-bytes [< | > | greater-than | less-than]** *number* **] [tx-packets [< | > | greater-than | less-than]** *number* **] [type** *flow_type* **] } [| { grep** *grep_options* **| more }]**

Web Element Manager Path

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

show active-charging sessions

This command displays the information for the active charging flows. The P2P protocol type flows now supports the following applications:

- Armagettron
- Blackberry
- Citrix
- Clubpenguin
- Crossfire
- Dofus

- Facebook
- Fiesta
- Florensia
- Funshion
- Guildwars
- Icecast
- ISAKMP
- Kontiki
- Maplestory
- Meebo
- MGCP
- Octoshape
- OFF
- PS3
- Real Media Stream
- Rfactor
- Shoutcast
- Splashfighter
- SSDP
- StealthNet
- STUN
- TeamSpeak
- Thunder
- Tor
- Truphone
- Veoh TV
- WII
- Windows Media Stream
- World of Kungfu
- XDCC
- YourFreedom

CLI (Exec Mode)

```
show active-charging flows { all | [ connected-time [ < | > | greater-than
| less-than ] seconds ] [ flow-id flow_id ] [ full ] [ idle-time [ < | > |
greater-than | less-than ] seconds ] [ ip-address  [ server | subscriber ]
[ < | > | IPv4 | greater-than | less-than ] address ] [ nat { not-required
| required [ nat-ip nat_ip_address ] } ] [ port-number [ server |
subscriber ] [ < | > | IPv4 | greater-than | less-than ] number ] [ rx-bytes
[ < | > | greater-than | less-than ] number ] [ rx-packets [ < | > |
greater-than | less-than ] number ] [ session-id session_id ] [ summary ] [
trans-proto { icmp | tcp | udp } ] [ tx-bytes [ < | > | greater-than |
```

```
less-than ] number ] [ tx-packets [ < | > | greater-than | less-than ]
number ] [ type flow_type ] } [ | { grep grep_options | more } ]
```

Web Element Manager Path

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

show active-charging analyzer statistics name p2p verbose

This command displays Active Charging protocol analyzer statistics for the P2P protocol analyzer. The following new fields are added to the output of this command to display the uplink/downlink bytes and uplink/downlink packets for the following protocols:

- Icecast
- Kontiki
- Meebo
- Shoutcast
- Truphone
- Thunder
- Armagettron
- Blackberry
- Citrix
- Clubpenguin
- Crossfire
- Dofus
- Fiesta
- Florensia
- Funshion
- Guildwars
- Isakmp
- Maplestory
- Mgcp
- Octoshape
- Off
- Ps3
- Rmstream
- Rfactor
- Splashfighter
- Ssdp
- Stealthnet
- Stun
- Teamspeak
- Tor

- Veohtv
- Wii
- Wmstream
- Wofkungfu
- Xdcc
- Yourfreetunnel
- Facebook

The following fields are modified in the output of this command to display the uplink/downlink bytes and uplink/downlink packets for the following protocols:

- Skype-non-audio
- Skype-audio
- Msn-video
- Msn-audio
- Msn-non-a/v
- Yahoo-non-audio
- Yahoo-audio
- Oscar-non-audio
- Oscar-audio
- Gtalk-non-audio
- Gtalk-audio

CLI (Exec Mode)

show active-charging analyzer statistics name p2p [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 type p2p

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

- Current ARMAGETTRON Sessions
- Current BLACKBERRY Sessions
- Current CITRIX Sessions
- Current CLUBPENGUIN Sessions
- Current CROSSFIRE Sessions
- Current DOFUS Sessions
- Current FIESTA Sessions
- Current FLORENSIA Sessions
- Current FUNSHION Sessions
- Current GUILDWARS Sessions

- Current ISAKMP Sessions
- Current MGCP Sessions
- Current OCTOSHAPE Sessions
- Current OFF Sessions
- Current PS3 Sessions
- Current RMSTREAM Sessions
- Current RFACTOR Sessions
- Current SPLASHFIGHTER Sessions
- Current SSDP Sessions
- Current STEALTHNET Sessions
- Current STUN Sessions
- Current TEAM SPEAK Sessions
- Current TOR Sessions
- Current VEOH TV Sessions
- Current WII Sessions
- Current WMSTREAM Sessions
- Current WOFKUNGFU Sessions
- Current XDCC Sessions
- Current YOURFREEDOM Sessions
- Current FACEBOOK Sessions
- Current MSN non-a/v Sessions

The following fields are modified in the output of this command:

- Current SKYPE audio Sessions
- Current SKYPE non-audio Sessions
- Current YAHOO audio Sessions
- Current YAHOO non-audio Sessions
- Current MSN audio Sessions
- Current MSN non-audio Sessions
- Current MSN video Sessions
- Current OSCAR audio Sessions
- Current OSCAR non-audio Sessions
- Current GTALK audio Sessions
- Current GTALK non-audio Sessions

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.

Serving Gateway Commands - Modified in Release 11.0

This section provides information about modified Serving Gateway (S-GW) commands.

clear egtpc

The following keywords have been added to this command:

- **interface-sgsn**
- **sgsn-address** *ip_address*

CLI (Exec Mode)

clear egtpc statistics [egtp-service *name* **| interface-type { interface-mme | interface-pgw-ingress | interface-sgsn | interface-sgw-egress | interface-sgwingress } | mme-address** *ip_address* **| pgw-address** *ip_address* **| sgsn-address** *ip_address* **| sgw-address** *ip_address* **]**

Web Element Manager Path

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

show egtpc peers

The following keyword has been added to this command:

sgsn

CLI (Exec Mode)

show egtpc peers [address *ip_address* **| egtp-service** *name* **] | interface { mme | pgw-ingress | sgsn | sgw-egress | sgw-ingress } [address** *ip_address* **] [wf1] }] [| { grep** *grep_options* **| more }]**

Web Element Manager Path

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

show egtpc sessions

The following keyword has been added to this command:

sgsn

CLI (Exec Mode)

show egtpc sessions [egtp-service *name* **| interface { mme | pgw-ingress | sgsn | sgw-egress | sgw-ingress }] [| { grep** *grep_options* **| more }]**

Web Element Manager Path

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

show egtpc statistics

The following keywords have been added to this command:

- **sgsn**
- **sgsn-address** *ip_address*

CLI (Exec Mode)

show egtpc statistics [egtp-service *name* **| interface { mme | pgw-ingress | sgsn | sgw-egress | sgw-ingess } | mme-address** *ip_address* **| pgw-address** *ip_address* **| sgsn-address** *ip_address* **| sgw-address** *ip_address* **] [verbose] [| { grep** *grep_options* **| more }]**

Web Element Manager Path

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

Session Control Manager Commands - Modified in Release 11.0

The following SCM commands have been modified in Release 11.0.

clear cscf service

This command resets statistics counters for a specific CSCF service, all CSCF services, or for all services within a specified context (VPN). The following keywords have been added to the **tcp** keyword:

- **msrp**: Clears statistics related to CSCF TCP MSRP statistics.
- **sip**: Clears statistics related to CSCF TCP SIP statistics.

CLI (Exec Mode)

clear cscf service { diameter { location-info | policy-control } statistics [servicename *service_name* **| vpn-name** *name* **] | li-packet-cable statistics [service-name** *service_name* **] | performance-counters name** *service_name* **| statistics name** *service_name* **{ all | calls | ip-security | message | package-name { message-summary | presence | reg | winfo } | registrations | sigcomp | tcp { msrp | sip } } }**

Web Element Manager Path

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

show cscf service

This command displays configuration and/or statistic information for CSCF services on the system. The following keywords have been added to the **tcp** keyword:

- **msrp**: Displays statistics related to CSCF TCP MSRP statistics.
- **sip**: Displays statistics related to CSCF TCP SIP statistics.

CLI (Exec Mode)

show cscf service { all [counters] | diameter { location-info statistics service-name *service_name* **[vpn-name** *name* **] | policy-control statistics servicename** *service_name* **[vpn-name** *name* **] } | grey-list name** *name* **| li-packet-cable statistics service-name** *service_name* **| performance-counters name** *service_name* **| statistics name** *service_name* **[all | calls | ip-security | message | package-name { message-summary | presence | reg | winfo } | registrations | sigcomp | tcp { msrp | sip }] | subscription name** *service_name* **} [| { grep** *grep_options* **| more }]**

Web Element Manager Path

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

SGSN Commands - Modified in Release 11.0

None for this release.

Obsoleted Commands

This section contains performance management commands that have been obsoleted in Release 11.0. Obsoleted commands in this version are divided into the following sections:

- *Common Commands - Obsoleted from Release 11.0*
- *Content Filtering Commands - Obsoleted from Release 11.0*
- *ECS Commands - Obsoleted from Release 11.0*
- *Firewall Commands - Obsoleted from Release 11.0*
- *GGSN Commands - Obsoleted from Release 11.0*
- *HA Commands - Obsoleted from Release 11.0*
- *NAT Commands - Obsoleted from Release 11.0*
- *PDSN Commands - Obsoleted from Release 11.0*
- *Peer-to-Peer Commands - Obsoleted from Release 11.0*
- *SGSN Commands - Obsoleted from Release 11.0*

Common Commands - Obsoleted from Release 11.0

The following common commands have been obsoleted in Release 11.0.

show ims-authorization policy-gate

This command has been deprecated in release 11.0 and later releases.

CLI (Exec Mode)

`show ims-authorization policy-gate`

Web Element Manager Path

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

show ims-authorization service name

The **`QoS Update Timeout`** field was removed from the output of **`show ims-authorization service name`** command in release 11.0 and later releases.

CLI (Exec Mode)

`show ims-authorization service name`

Web Element Manager Path

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

show ims-authorization service statistics

The following fields were removed from the output of **`show ims-authorization service statistics`** command in release 11.0 and later releases:

- TFT Delete
- Packet Statistics
  - Uplink Pkt Processed
  - Downlink Pkt Processed
  - Uplink Bytes Processed
  - Downlink Bytes Processed
  - Uplink Pkt Dropped
  - Downlink Pkt Dropped
  - Uplink Bytes Dropped
  - Downlink Bytes Dropped

CLI (Exec Mode)

`show ims-authorization service statistics`

Web Element Manager Path

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

show ims-authorization sessions full

The following fields were removed from the output of **`show ims-authorization sessions full`** command in release 11.0 and later releases:

- Charging Rules
- Session Packet Statistics
  - Uplink Pkt Processed
  - Downlink Pkt Processed
  - Uplink Bytes Processed
  - Downlink Bytes Processed
  - Uplink Pkt Dropped
  - Downlink Pkt Dropped
  - Uplink Bytes Dropped
  - Downlink Bytes Dropped

CLI (Exec Mode)

`show ims-authorization session full`

Web Element Manager Path

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

Content Filtering Commands - Obsoleted from Release 11.0

None for this release.

ECS Commands - Obsoleted from Release 11.0

None for this release.

Firewall Commands - Obsoleted from Release 11.0

The following Stateful Firewall commands have been obsoleted in Release 11.0.

show active-charging subsystem all

The following fields were removed from the output of **`show active-charging subsystem all`** command in release 11.0 and later releases:

- Total Firewall Subscribers
- Total NAT Subscribers

CLI (Exec Mode)

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

Web Element Manager Path

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

GGSN Commands - Obsoleted from Release 11.0

None for this release.

HA Commands - Obsoleted from Release 11.0

None for this release.

NAT Commands - Obsoleted from Release 11.0

None for this release.

PDSN Commands - Obsoleted from Release 11.0

None for this release.

Peer-to-Peer Commands - Obsoleted from Release 11.0

None for this release.

SGSN Commands - Obsoleted from Release 11.0

None for this release.

GTPP Storage Server Changes

None for this release.

Web Element Manager Changes

There were no Web Element Manager changes in Release 11.0.

CHAPTER 6
SECURITY MANAGEMENT

This section contains additions and changes made to the security features available in Release 11.0.

Security Enhancements

New Commands

None for this release.

Modified Commands

None for this release.

Obsoleted Commands

None for this release.