Release 8.x to Release 9.0 Change Reference

Version 9.0

Generally Available 06-30-2010

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

Text Part Number: OL-22957-01

Release 8.x to Release 9.0 Change Reference

TABLE OF CONTENTS

About This Guide

Conventions Used xii
Contacting Customer Support xiv

Chapter 1: New Feature Summary

Related Documents 1-2
Common Features in Release 9.0 1-3
Dynamic MPLS Label Support 1-3
Benefits 1-3
Description 1-3
License Keys 1-3
Side-by-side Redundancy for the 10 Gig Line Card (XGLC) 1-3
Packet Processor Card (PPC) 1-4
DCCA URCS (IPC-G) Steering Based on Subscriber IMSI Prefix/Suffix 1-5
EDR/UDR File Push Directory Structure 1-5
3GPP R7 Gx Interface Support 1-6
Bearer ID in Bearer-level QoS Information 1-6
Bearer ID Validation 1-6
Failure Handling Action 1-6
Gn APN in Gx Messages 1-7
Maximum Number of Charging-Rule-Definition AVPs Supported in a Single CCA 1-7
Provisioning of Event Triggers 1-7
Rejection of Unauthorized Gx Messages 1-7
ASN GW Features in Release 9.0 1-8
Content Filtering in Release 9.0 1-9
Category-based Static-and-Dynamic Content Filtering 1-9
ECS Features in Release 9.0 1-10
EDR Generation in Flow-end and Transaction Complete Scenarios with sn-volume Fields 1-10
IPv6 and ICMPv6 Support in Enhanced Charging Service 1-11
URL Filtering 1-11
eHRPD Features in Release 9.0 1-12
New HSGW Features 1-12
New P-GW Features 1-12
ESS Features in Release 9.0 1-14
Generic L-ESS 1-14
Firewall Features in Release 9.0 1-15
Per Subscriber Stateful Firewall Licensing 1-15
GGSN Features in Release 9.0 1-16
GRE Protocol Interface 1-16
Overcharging Protection on Loss of Radio Coverage 1-18

GSS Features in Release 9.0 1-19
Multiple Instance GSS 1-19
Monitoring of Disk Partitions 1-19
HA Features in Release 9.0 1-21
inPilot Features in Release 9.0 1-22
Bulkstat and KPI Reports 1-22
Exporting Reports to PDF Format 1-22
GUI/Console based Installation 1-22
Log File Path 1-22
RAT Classification Report 1-22
Supported File System 1-23
Voice Call Duration Reports 1-23
IP Services Gateway Features in Release 9.0 1-24
LTE/SAE Features in Release 9.0 1-25
New P-GW Features 1-25
New MME Features 1-25
New S-GW Features 1-26
NAT Features in Release 9.0 1-27
NAT Licensing 1-27
PDG/TTG Features in Release 9.0 1-28
PDIF Features in Release 9.0 1-29
Multiple Traffic Selectors 1-29
Selective Diameter Profile Update Request Control 1-29
PDSN Features in Release 9.0 1-30
Peer-to-Peer Features in Release 9.0 1-31
Dynamic P2P Signature Updates 1-31
P2P Protocols Detection Support 1-31
SCM Features in Release 9.0 1-33
IPv4-IPv6 Interworking 1-33
SGSN Features in Release 9.0 1-36
Configurable Gf IMEI Check Event Timer 1-36
Default APN 1-36
Disable Signaling Indication IE in RANAP messages 1-36
Limiting Iu Connections in RANAP Messages 1-37
Limits / Engineering Rules 1-37
Lawful Intercept 1-37
Local QoS Capping 1-38
Multiple PLMN Support 1-38
Overcharging Protection 1-38
PSC2 - Packet Services Card 2 1-39
Suppression of Paging Cause IE in Paging Request 1-39
Tracking Usage of GPRS Encryption Algorithm 1-39
XGLC - 10 Gigabit Ethernet Line Card 1-40

Web Element Manager Features in Release 9.0 1-41

Chapter 2: Fault Management

SNMP MIB Objects in Release 9.0 2-2
New Objects 2-2
Modified Objects 2-7
Obsoleted Objects 2-7
Deleted Objects 2-7
New Alarms 2-7
Modified Alarms 2-7
Obsoleted Alarms 2-8
Deleted Alarms 2-8
Web Element Manager Path 2-8
Content Filtering MIB Objects for Release 9.0 2-9
New Objects 2-9
Modified Objects 2-9
Obsoleted Objects 2-9
Deleted Objects 2-9
New Alarms 2-9
Modified Alarms 2-9
Obsoleted Alarms 2-9
Deleted Alarms 2-9
Web Element Manager Path 2-9
ESS MIB Objects for Release 9.0 2-10
New Objects 2-10
Modified Objects 2-10
Obsoleted Objects 2-10
Deleted Objects 2-10
New Alarms 2-10
Modified Alarms 2-10
Obsoleted Alarms 2-10
Deleted Alarms 2-10
Intelligent Packet Monitoring Systems (IPMS) MIB in Release 9.0 2-11
New Objects 2-11
Modified Objects 2-11
Obsoleted Objects 2-11
Deleted Objects 2-11
New Alarms 2-11
Modified Alarms 2-11
Obsoleted Alarms 2-11
Deleted Alarms 2-11
Web Element Manager Path 2-11
Web Element Manager Enhancements in Release 9.0 2-12
New Objects 2-12
Modified Objects 2-12
Obsoleted Objects 2-12

Deleted Objects 2-12
New Alarms 2-12
Modified Alarms 2-12
Obsoleted Alarms 2-12
Deleted Alarms 2-12
Web Element Manager Path 2-12

Chapter 3: Configuration Management

New Configuration Commands 3-2
Common Commands - New in Release 9.0 3-2
apn-name-to-be-included 3-2
cdr-multi-mode 3-2
ip vrf 3-3
ip vrf 3-3
ip vrf forwarding 3-3
radius ip vrf 3-3
radius ip vrf 3-4
radius accounting billing-version 3-4
radius attribute 3-4
ASN GW Commands - New in Release 9.0 3-5
Content Filtering Commands - New in Release 9.0 3-6
ECS Commands - New in Release 9.0 3-7
edr voip-call-end 3-7
group-of-prefixed-urls 3-7
group-of-ruledefs-application 3-7
icmp req-threshold 3-7
icmpv6 any-match 3-8
icmpv6 code 3-8
icmpv6 type 3-8
ip version 3-8
system-limit 3-8
policy-control burst-size 3-9
post-processing dynamic 3-9
prefixed-url 3-9
url-preprocessing 3-9
Firewall Commands - New in Release 9.0 3-11
firewall icmp-checksum-error 3-11
firewall icmp-fsm 3-11
firewall ip-reassembly-failure 3-11
firewall malformed-packets 3-11
firewall tcp-checksum-error 3-12
firewall tcp-fsm 3-12
firewall tcp-options-error 3-12
firewall tcp-syn-with-ecn-cwr 3-12
firewall udp-checksum-error 3-13
firewall validate-ip-options 3-13

GGSN Commands - New in Release 9.0 3-14
gtpc nsapi-in-create-pdp-response 3-14
gtpc ran-procedure-ready-delay 3-14
gtpc private-extension 3-15
HA Commands - New in Release 9.0 3-16
NAT Commands - New in Release 9.0 3-17
firewall tcp-idle-timeout-action 3-17
nat private-ip-flow-timeout 3-17
secondary ip pool 3-17
PDIF Commands - New in Release 9.0 3-18
PDSN Commands - New in Release 9.0 3-18
l2tp send accounting-correlation-info 3-18
Peer-to-Peer - New in Release 9.0 3-19
p2p-dynamic-rules 3-19
Session Control Manager Commands - New in Release 9.0 3-20
ipv4-ipv6-interworking 3-20
sip-request 3-20
SGSN Commands - New in Release 9.0 3-21
apn-selection-default 3-21
gtp 3-21
gtpp trigger rat-change 3-21
override-arp-with-ggsn-arp 3-21
ranap 3-22
loss-of-radio-coverage ranap-cause 3-22
ranap 3-22
reset-resource 3-23
gtpp dead-server suppress-cdrs 3-23
inbound-asp-identifier validate 3-23
Modified Configuration Commands 3-24
Common Commands - Modified in Release 9.0 3-24
configure hd raid 3-24
diameter peer-select 3-24
ip arp 3-25
ip route 3-25
ospf graceful-restart 3-25
policy-control charging-rule-base-name 3-25
require active-charging 3-26
radius accounting 3-26
snmp target 3-27
tunnel-mode 3-27
Content Filtering Commands - Modified in Release 9.0 3-28
content-filtering mode 3-28
upgrade content-filtering category rater-pkg 3-28
ECS Commands - Modified in Release 9.0 3-29
billing-records 3-29
ftp command id 3-29

ftp command name 3-29
ip dst-address 3-30
ip protocol 3-30
ip protocol 3-30
rule-variable 3-32
Firewall Commands - Modified in Release 9.0 3-33
GGSN Commands - Modified in Release 9.0 3-34
gtpp storage-server local file 3-34
authentication 3-34
HA Commands - Modified in Release 9.0 3-35
NAT Commands - Modified in Release 9.0 3-36
access-rule 3-36
ip pool 3-36
PDIF Commands - Modified in Release 9.0 3-38
control-dont-fragment 3-38
PDSN Commands - Modified for Release 9.0 3-39
Peer-to-Peer - Modified for Release 9.0 3-40
p2p-detection protocol 3-40
p2p-detection protocol 3-40
show active-charging analyzer statistics 3-41
show active-charging flows 3-42
show active-charging sessions 3-42
p2p protocol 3-43
Session Control Manager Commands - Modified for Release 9.0 3-45
bind 3-45
diameter 3-45
SGSN Commands - Modified for Release 9.0 3-46
gmm 3-46
llc 3-46
llc 3-46
rnc id 3-47
qos prefer-as-cap 3-47
apn/apn-selection-default/wildcard-apn 3-47
application-context-name 3-47
Obsoleted Commands 3-48
Common Commands - Obsoleted in Release 9.0 3-48
css acsmgr-selection-attempts 3-48
css delivery-sequence 3-48
css service 3-49
css server 3-49
redirect css delivery-sequence 3-49
redirect css delivery-sequence 3-49
Content Filtering Commands - Obsoleted in Release 9.0 3-50
ECS Commands - Obsoleted in Release 9.0 3-51
Firewall Commands - Obsoleted in Release 9.0 3-52
firewall tcp-first-packet-non-syn 3-52

GGSN Commands - Obsoleted in Release 9.0 3-53
HA Commands - Obsoleted in Release 9.0 3-54
PDSN Commands - Obsoleted in Release 9.0 3-55
SGSN Commands - Obsoleted in Release 9.0 3-56
authenticate attach 3-56
authenticate rau update-type 3-56
GTPP Storage Server (GSS) 3-57
GSS Changes in Release 9.0 3-57
Web Element Manager Changes 3-58

Chapter 4: Accounting Management

Bulk Statistic Enhancements in Release 9.0 4-2
New Bulk Statistics 4-2
APN Schema 4-2
CSCF Schema 4-2
DCCA Schema 4-7
DPCA Schema 4-8
eGTP-C Schema 4-8
GPRS Schema 4-8
MIPv6HA Schema 4-9
P-GW Schema 4-9
S-GW Schema 4-9
System Schema 4-9
SGSN Schema 4-10
Modified Bulk Statistics 4-11
Obsoleted Bulk Statistics 4-11
SGSN Schema 4-11
SGTP Schema: 4-11
Web Element Manager Path 4-11
CDR Enhancements 4-12
IPv6 Support in S-CDRs in custom11 4-12
SGSN Support for custom17 4-12
Command Enhancements 4-13
New Commands 4-14
RADIUS Attributes in Release 9.0 4-15
New Attributes 4-15
Modified Attributes 4-15
Removed Attributes 4-16
Diameter Attributes in Release 9.0 4-17
New Attributes 4-17
Modified Attributes 4-21
Removed Attributes 4-22
Web Element Manager Enhancements 4-23

Chapter 5: Performance Management

New Commands 5-2
Common Commands - New in Release 9.0 5-2
Content Filtering Commands - New in Release 9.0 5-3
ECS Commands - New in Release 9.0 5-4
Firewall Commands - New in Release 9.0 5-5
GGSN Commands - New in Release 9.0 5-6
show apn counter ip-allocation 5-6
show ip interface 5-6
HA Commands - New in Release 9.0 5-7
NAT Commands - New in Release 9.0 5-8
PDIF Commands - New in Release 9.0 5-9
PDSN Commands - New in Release 9.0 5-10
Peer-to-Peer - New in Release 9.0 5-11
show active-charging p2p-dynamic-rules 5-11
SGSN Commands - New in Release 9.0 5-12
Modified Commands 5-13
Common Commands - Modified in Release 9.0 5-13
clear active-charging credit-control statistics 5-13
clear crypto 5-13
clear ims-authorization policy-control 5-14
monitor protocol 5-14
monitor subscriber username 5-14
show active-charging credit-control 5-14
show active-charging fw-and-nat policy name 5-15
show ims-authorization policy-control 5-15
show rohc 5-16
Content Filtering Commands - Modified in Release 9.0 5-17
clear content-filtering category statistics 5-17
show active-charging content-filtering category statistics 5-17
show active-charging content-filtering server-group statistics 5-18
show content-filtering category database facility srdbmgr 5-18
show content-filtering category statistics facility srdbmgr 5-18
show content-filtering category url <url> policy-id <id> verbose 5-19
show active-charging content-filtering category statistics 5-19
show content-filtering category statistics facility srdbmgr all 5-19
show active-charging content-filtering category statistics 5-20
ECS Commands - Modified in Release 9.0 5-21
show active-charging service 5-21
show active-charging analyzer statistics 5-21
show active-charging analyzer statistics name 5-22
show active-charging analyzer statistics name dns 5-22
show active-charging sessions full all 5-23
show active-charging flows type 5-23
show active-charging flows ip-address 5-23
show active-charging rulebase statistics 5-24

Firewall Commands - Modified in Release 9.0 5-25
show active-charging firewall statistics verbose 5-25
GGSN Commands - Modified in Release 9.0 5-26
show subscribers ggsn-only summary 5-26
show subscribers ggsn-only full 5-26
show gtpc full 5-26
show gtpc statistics 5-26
HA Commands - Modified in Release 9.0 5-28
NAT Commands - Modified in Release 9.0 5-29
PDIF Commands - Modified in Release 9.0 5-30
PDSN Commands - Modified in Release 9.0 5-31
Peer-to-Peer Commands - Modified in Release 9.0 5-32
show active-charging rulebase statistics name 5-32
show active-charging analyzer statistics name p2p verbose 5-32
show active-charging sessions summary 5-33
show active-charging sessions summary type p2p 5-33
Session Control Manager Commands - Modified in Release 9.0 5-35
SGSN Commands - Modified in Release 9.0 5-36
Obsoleted Commands 5-37
Common Commands - Obsoleted from Release 9.0 5-37
show css delivery-sequence 5-37
show css server 5-37
show css service 5-37
Content Filtering Commands - Obsoleted from Release 9.0 5-38
ECS Commands - Obsoleted from Release 9.0 5-38
Firewall Commands - Obsoleted from Release 9.0 5-38
GGSN Commands - Obsoleted from Release 9.0 5-38
HA Commands - Obsoleted from Release 9.0 5-38
NAT Commands - Obsoleted from Release 9.0 5-38
PDSN Commands - Obsoleted from Release 9.0 5-38
Peer-to-Peer Commands - Obsoleted from Release 9.0 5-39
SGSN Commands - Obsoleted from Release 9.0 5-39
GTPP Storage Server Changes 5-40
show gtpp storage-server status 5-40
show gtpp storage-server streaming file statistics 5-40
show gtpp storage-server streaming file statistics verbose 5-40
Web Element Manager Changes 5-42

Chapter 6: Security Management

Security Enhancements 6-2
New Commands 6-2
Modified Commands 6-2
Obsoleted Commands 6-2

ABOUT THIS GUIDE

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

Conventions Used

The following tables describe the conventions used throughout this documentation.

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

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

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

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

Contacting Customer Support

Use the information in this section to contact customer support.

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

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

IMPORTANT

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

CHAPTER 1
NEW FEATURE SUMMARY

This guide identifies features and functionality added or modified between software releases 8.x and 9.0. Topics covered in this chapter are:

- *Common Features in Release 9.0*
- *ASN GW Features in Release 9.0*
- *Content Filtering in Release 9.0*
- *ECS Features in Release 9.0*
- *eHRPD Features in Release 9.0*
- *ESS Features in Release 9.0*
- *Firewall Features in Release 9.0*
- *GGSN Features in Release 9.0*
- *GSS Features in Release 9.0*
- *HA Features in Release 9.0*
- *inPilot Features in Release 9.0*
- *IP Services Gateway Features in Release 9.0*
- *LTE/SAE Features in Release 9.0*
- *NAT Features in Release 9.0*
- *PDIF Features in Release 9.0*
- *PDSN Features in Release 9.0*
- *Peer-to-Peer Features in Release 9.0*
- *SCM Features in Release 9.0*
- *SGSN Features in Release 9.0*
- *Web Element Manager Features in Release 9.0*

Related Documents

Additional information on these items is located in the documents provided with the 9.0 release, see the table below.

Table 1-1 Cisco ASR 5000 Series 9.0 Release Documentation

Document	Part Number
Release 8.x to 9.0 Change Reference	OL-22957-01
Product Overview Guide	OL-22937-01
Aggregation Services Router Installation and Administration Guide	OL-22995-01
Cisco Web Element Manager Installation and Administration Guide	OL-22945-01
SNMP MIB Reference Manual	OL-22941-01
AAA Interface Administration and Reference	OL-22955-01
GTPP Storage Server Installation and Administration Guide	OL-22950-01
Thresholding Configuration Guide	OL-22966-01
Statistics and Counters Reference	OL-22990-01
Command Line Interface Reference	OL-22947-01
System Administration Guide	OL-22969-01
Enhanced Feature Configuration Guide	OL-22982-01
Gateway GPRS Support Node Administration Guide	OL-22943-01
Serving GPRS Support Node Administration Guide	OL-22978-01

Table 1-2 Starent ST40 Series 9.0 Release Documentation

Document	Part Number
PDSN Administration Guide	901-00-0003 Z
Command Line Interface Reference	901-00-0014 AT
Enhanced Charging Service Administration Guide	901-00-0038 X
SCM Administration Guide	901-00-0041 E
Content Filtering Services Administration Guide	901-00-0056 J
Peer-to-Peer Detection Administration Guide	901-00-0057 M
Packet Data Interworking Function Administration Guide	901-00-0059 L
Personal Stateful Firewall Administration Guide	901-00-0060 N
PDG/TTG Administration Guide	901-00-0093 B
PHS Gateway Administration Guide	901-00-0075 E
HRPD Serving Gateway Administration Guide	901-00-0076 A
PDN Gateway Administration Guide	901-00-0077 A
Serving Gateway Administration Guide	901-00-0078 A
Mobility Management Entity Administration Guide	901-00-0079 A
NAT Administration Guide	901-00-0086 D
InPilot Installation and Administration Guide	901-00-0087 A

Common Features in Release 9.0

This section provides information on new features that are common to products in Release 9.0.

Dynamic MPLS Label Support

Benefits

This feature provides dynamic MPLS label support for ingress and egress traffic where system works as MPLS-Customer Edge system and maintains VRF routes in various VRFs and exchanges route information with peer over MP-eBGP session with an Autonomous System Border Router (ASBR).

Description

In deployment scenario the MPLS-CE system maintains VRF routes in various VRFs and exchanges route information with peer over MP-eBGP session with peer. The peer in this scenario is not a PE router but an ASBR. The ASBR does not need to maintain any VRF configuration. The PE routers use IBGP to redistribute labeled VPN-IPv4 routes either to an Autonomous System Border Router (ASBR), or to a route reflector of which an ASBR is a client. The ASBR then uses eBGP to redistribute those labeled VPN-IPv4 routes to MPLS-CE in another AS. Because of eBGP connection, ASBR changes the next-hop and labels in the routes learnt from iBGP peers before advertising to MPLS-CE. MPLS-CE is directly connected eBGP peering and uses only MP-eBGP to advertise and learn routes. MPLS-CE pushes/pops single label to/from ASBR, which is learnt over MP-eBGP connection. This scenario uses dynamic MPLS label and avoids configuration of VRFs on PE, which are already configured on MPLS-CE.

For more information on functioning and configuration of this interface, refer *Multiple Protocol Lable Switching* chapter in *System Enhanced Feature Configuration Guide*.

License Keys

Requires separate license key.

Side-by-side Redundancy for the 10 Gig Line Card (XGLC)

Starent chassis provides the redundancy scheme for using top and bottom line card slots for one-to-one redundancy for line cards with top and bottom line card slot for one-to-one redundancy.

The XGLC is a full-height card that requires both top and bottom line card slots for a single 10-gigabit port. This means that the scheme for using top and bottom line card slots for one-to-one redundancy is not workable for XGLCs. To achieve one-to-one line card redundancy, user must install two XGLCs in adjacent slots. Otherwise, user can configure port and card redundancy for the XGLCs in the same way as other line cards. There are no restrictions that prevent the side-to-side 1:1 XGLC redundant arrangement from functioning with other Ethernet line card types.

Each PSC or PSC2 is mated to a single XGLC. Monitoring functions occur in a distributed fashion. Select the line cards that act as a redundant pair via the CLI. Configure the

redundant pairs prior to configuring the interface bindings so that proper parallel physical and logical port configurations are established. The card redundancy and monitoring begins as soon as the PSC or PSC2 in front is active.

Note: Side-by-side 1:1 redundancy only operates on top line card slot numbers: cards 17 through 23 and 26 through 32. Make sure that both PSCs or PSC2s in front of the line cards are of the same type, configured as a redundant pair, and active.

For more information on side by side 1:1 redundancy for 10 Gig line card (XGLC), refer *ST40 Hardware Installation Guide*.

Packet Processor Card (PPC)

The PPC has features a quad-core x86 2.5Ghz CPU and 16GB of RAM. The processor runs a single copy of the operating system. To check the CPU in the CLI, use the **`show cpu table`** command. The operating system running on the PPC treats the dual-core processor as a 2-way multi-processor. You can see this in the output of the **`show cpu info verbose`** command.

IMPORTANT

For this release, the PPC is limited to CDMA and HA functionality.

A second-generation data transport fixed programmable gate array (DT2 FPGA, abbreviated as DT2) connects the PPC's NPU bus to the switch fabric interface. The FPGA also provides a bypass path between the line card or Redundancy Crossbar Card (RCC) and the switch fabric for ATM traffic. Traffic from the line cards or the RCC is received over the FPGA's serial links and is sent to the NPU on its switch fabric interface. The traffic destined for the line cards or RCC is diverted from the NPU interface and sent over the serial links.

DT2 FPGA also connects to the control processors subsystem via a PCI-E bus. The PCI-E interface allows the control processors to perform register accesses to the FPGA and some components attached to it, and also allows DMA operations between the NPU and the control processors' memory. A statistics engine is provided in the FPGA. Two reduced latency DRAM (RLDRAM) chips attached to the FPGA provide 64MB of storage for counters.

The PPC has a 2.5 G/bps-based security processor that provides the highest performance for cryptographic acceleration of next-generation IP Security (IPsec), Secure Sockets Layer (SSL) and wireless LAN/WAN security applications with the latest security algorithms.

Redundancy

- The PPC is fully redundant with a spare PPC.

Capacity

- 3 million SAU and 6 million PDP contexts
- 2 million PDSN sessions
- 6 million HA sessions

Power Estimate

- 325W Maximum

DCCA URCS (IPC-G) Steering Based on Subscriber IMSI Prefix/Suffix

This release supports peer selection using IMSI prefix or suffix, or IMSI prefix or suffix range. Subscribers are now assigned to a primary OCS instance based on the IMSI prefix or suffix of a length of 1 to 15 digits. If the prefix or suffix keyword is not specified, the suffix will be considered. Up to 64 peer selects can be configured. At any time, either prefix or suffix mode can be used in one DCCA config. If the prefix or suffix mode is used, the lengths of all prefix/suffix must be equal.

EDR/UDR File Push Directory Structure

In earlier StarOS 9.0 releases, whenever CDR transfer mode push was configured with a remote URL, on the external server the chassis would by default create an extra directory in the base directory path before creating the edr/udr directories.

For example, with the following configuration:

```
cdr transfer-mode push primary url sftp://root:sn@1.2.3.4/<base_directory>
   cdr push-interval 60
   cdr remove-file-after-transfer
   cdr use-harddisk
```

The following directory structure was created on the external server:

```
<base_directory>
   | <chassis1_host_name>
      | edr
      | udr
   | <chassis2_host_name>
      | edr
      | udr
```

This enabled to keep EDR and UDR files from multiple chassis pushing to the same external server with same base directory separate.

In the current release, the default behavior has changed, the extra directory with the chassis host name will not be created on the external server. This behavior is the same as in the StarOS 8.x releases. The directory structure will be:

```
<base_directory>
   | edr
   | udr
```

3GPP R7 Gx Interface Support

As defined by the 3GPP standards, the R7 Gx interface is located between the GGSN and the Policy Decision Function (PDF) / Policy and Charging Rule Function (PCRF). It is a Diameter-based interface and provides the functions provided earlier by the Gx (R6) and Go interfaces. Gx interface as part of a Policy / PCC framework allows the operator to have dynamic policy and charging control, key features when “flat rate” broadband services are offered. However, it is paramount that the operator maintains control over the available resources, and provides a fair usage policy to its subscribers, via bandwidth control, quota management and other mechanisms.

This release supports the following features:

- PCEF-based bearer binding
- IMSA support for secondary contexts
- QoS Negotiation AVP and QoS Upgrade AVP in Gx messages
- Single repository of ruledefs for all PDP contexts
- Moving of PCC rules across PDP contexts if indicated by PCRF
- QoS enforcement per service data flow
- Bearer identifier value extensible to non-GPRS access type
- Ability to define static policies to deny and allow based on 5-tuple information; ability to enable and disable from the PCRF

Bearer ID in Bearer-level QoS Information

In previous releases, in case of PCRF-based binding, when the bearer-level QoS information was received from PCRF without bearer ID, the UPC request with the change in QoS was sent to the default bearer.

In this release, this behavior has changed. In case of PCRF-based binding, the bearer ID is expected as part of the bearer-level QoS information from the PCRF. Otherwise the QoS information is ignored.

Bearer ID Validation

In previous releases, the bearer ID in the QoS-Information AVP from the PCRF was not being validated at the PCEF.

In this release, the bearer ID is validated and if found to be invalid is ignored.

Failure Handling Action

In StarOS 8.1 and earlier releases, when the failure handling action configured under the IMSA service is terminate, and if the primary server is down but the secondary server is up during call establishment, the call is terminated.

In this release, this behavior has changed, the call is established with the secondary server.

Gn APN in Gx Messages

In StarOS 8.0, if in the APN configuration both the virtual APN name and Gn APN name are configured, the virtual APN name is sent in the Gx messages.

In this release, if both the virtual APN name and Gn APN name are configured, the Gn APN name is sent in the Gx messages. In case only the Gn APN name is configured, the Gn APN name is sent.

Maximum Number of Charging-Rule-Definition AVPs Supported in a Single CCA

In previous releases, there was no limit check for the number of Charging-Rule-Definition AVPs (dynamic rules) that are processed in a single Gx CCA command. In StarOS 9.0, the number of dynamic rules is limited to 100 per Gx message.

In this release, the following per Gx message limits are applicable:

- Charging-Rule-Names: 256
- Charging-Rule-Base-Names: 20
- Charging-Rule-Definitions: 100
- Length of Charging-rule-name/base-name: 32

Provisioning of Event Triggers

In this release, whenever the PCRF subscribes to one or more event triggers by using the RAR command, the PCEF sends the corresponding currently applicable values (e.g. 3GPP-SGSN-Address AVP or 3GPP-SGSN-IPv6-Address AVP, RAT-Type, 3GPP-User-Location-Info, etc.) to the PCRF in the RAA if available, and in this case, the Event-Trigger AVPs will not be included.

Rejection of Unauthorized Gx Messages

In StarOS 8.1, if PCRF does not authorize the requested QoS values, the PCEF does not reject the Gx response messages.

In StarOS 9.0, if the PCRF does not authorize the requested QoS values, or if QoS values previously authorized by the PCRF are not available, the PCEF rejects the Gx messages from PCRF and the corresponding access side procedure. The Max Uplink/Downlink, Guaranteed Uplink/Downlink parameters are considered to check whether the QoS values are authorized or not. Validation is done across all Gx messages.

ASN GW Features in Release 9.0

This section provides information for new features in the ASN GW Service in Release 9.0.

None for this release.

Content Filtering in Release 9.0

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

Category-based Static-and-Dynamic Content Filtering

This release introduces support for Category-based Static-and-Dynamic Content Filtering, wherein if static rating categorizes a URL as either “dynamic” or “unknown”, the “requested content” is sent for dynamic rating. Wherein the “requested content” is analyzed and categorized. Action is taken based on the category determined by dynamic rating, and the action configured for that category in the subscriber’s content filtering policy. Possible actions include permitting, blocking, redirecting, and inserting/altering content.

Dynamic Content Filtering enables on-the-fly content analysis of Web traffic using different content analysis techniques. When a Web page is received, it is analyzed and then categorized according to the content found in the page. Whether a Web site has existed for five months or for five minutes does not matter since determination of the category to which the Web page belongs is made just at the time of request. A combination of static filtering and dynamic inspection provides real accuracy and scalability as the Web weaves an increasingly sophisticated network of sites.

IMPORTANT

Category-based Content Filtering can only work in static-only or in static-and-dynamic modes. Dynamic-only Content Filtering mode is not supported.

For more information, refer to the *Content Filtering Services Administration Guide*.

ECS Features in Release 9.0

This section provides information on new features in the Enhanced Charging Service in Release 9.0.

EDR Generation in Flow-end and Transaction Complete Scenarios with sn-volume Fields

In this release sn-volume-amt counters will be re-initialized only when the fields are populated in EDRs. For example, consider the following two EDR formats:

```
edr-format edr1
   rule-variable http url priority 10
   attribute sn-volume-amt ip bytes uplink priority 500
   attribute sn-volume-amt ip bytes downlink priority 510
   attribute sn-volume-amt ip pkts uplink priority 520
   attribute sn-volume-amt ip pkts downlink priority 530
   attribute sn-app-protocol priority 1000
   exit
edr-format edr2
   rule-variable http url priority 10
   attribute sn-app-protocol priority 1000
   exit
```

Previously, if edr2 was generated, even though sn-volume-amt fields are not populated, sn-volume-amt counters (uplink bytes, uplink packets, downlink bytes, downlink packets) were re-initialized. So the total volume reflected by EDRs in sn-volume-amt counters was less than the actual count.

In this release, sn-volume-amt counters will be re-initialized only if these fields are populated in the EDRs. Now, if edr2 is generated, these counters will not be re-initialized. These will be re-initialized only when edr1 is generated.

Also, note that only those counters will be re-initialized which are populated in EDR. For example, in the following EDR format:

```
edr-format edr3
   rule-variable http url priority 10
   attribute sn-volume-amt ip bytes uplink priority 500
   attribute sn-volume-amt ip bytes downlink priority 510
   attribute sn-app-protocol priority 1000
   exit
```

If edr3 is generated, only uplink bytes and downlink bytes counters will be re-initialized and uplink packets and downlink packets will contain the previous values till these fields are populated (say when edr1 is generated).

IPv6 and ICMPv6 Support in Enhanced Charging Service

StarOS 9.0 introduces support for IPv6 and ICMPv6 packets and their parsing in the Enhanced Charging Service.

ECS can now parse both IPv4 and IPv6 packets and pass them to upper layers for analysis. ECS will match the rule based on IPv6 fields and generate various statistics for IPv6 packets. Dynamic routing used by various analyzers like FTP, RTSP, RTP, and SIP also supports IPv6 addresses.

The enhancement to ECS in Release 9.0 provides appropriate CLIs to configure IPv6 fields in rules and EDRs. Various CLIs are provided to configure rules related to IPv6 fields for charging and routing. Several fields in EDRs give IP address. ECS will also support IPv6 addresses in these EDR fields. Show command CLIs which show IP addresses support IPv6 addresses as well. The various logs in ECS which log IP addresses along with other information, supports IPv6 addresses as well. ECS supports various header fields of IPv6 in EDRs. In config-acs-edr mode, ECS supports generating EDRs for IPv6 fields.

StarOS 9.0 also supports ICMPv6 packets and their parsing in ECSv2. The header structure of ICMP and ICMPv6 is similar but the values of header fields like type and code have different meaning in the two.

With the support for IPv6 in ECS, AAAA record type is now supported in DNS for IPv6 addresses.

URL Filtering

This release supports the URL Filtering feature, which simplifies using rule definitions for URL detection. Prefixed URLs are URLs of the proxies. A packet can have a URL of the proxy and the actual URL contiguously. First a packet is searched for the presence of proxy URL. If the proxy URL is found, it is truncated from the parsed information and only the actual URL (that immediately follows it) is used for rule matching and EDR generation.

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

eHRPD Features in Release 9.0

This section contains information on new 9.0 features that pertain to the HRPD Serving Gateway (HSGW) and the PDN Gateway (P-GW) supporting eHRPD network services.

New HSGW Features

The HSGW is new in release 9.0.

The HSGW terminates the eHRPD access network interface from the Evolved Access Network/Evolved Packet Core Function (eAN/ePCF) and routes UE-originated or terminated packet data traffic. It provides interworking with the eAN/ePCF and the PDN Gateway (P-GW) within the Evolved Packet Core (EPC) or LTE/SAE core network and performs the following functions:

- Mobility anchoring for inter-eAN handoffs
- Transport level packet marking in the uplink and the downlink, e.g., setting the DiffServ Code Point, based on the QCI of the associated EPS bearer
- Uplink and downlink charging per UE, PDN, and QCI
- Downlink bearer binding based on policy information
- Uplink bearer binding verification with packet dropping of UL traffic that does not comply with established uplink policy
- MAG functions for S2a mobility (i.e., Network-based mobility based on PMIPv6)
- Support for IPv4 and IPv6 address assignment
- EAP Authenticator function
- Policy enforcement functions defined for the Gxa interface
- Robust Header Compression (RoHC)
- Support for VSNCP and VSNP with UE
- Support for packet-based or HDLC-like framing on auxiliary connections
- IPv6 SLACC support, generating RAs responding to RSs

New P-GW Features

The P-GW is new in Release 9.0.

The P-GW terminates the SGi interface towards the Packet Data Network (PDN). If a UE is accessing multiple PDNs, there may be more than one P-GW for that UE. The P-GW provides connectivity to the UE to external packet data networks by being the point of exit and entry of traffic for the UE. A UE may have simultaneous connectivity with more than one P-GW for accessing multiple PDNs. The P-GW performs policy enforcement, packet filtering for each user, charging support, lawful interception and packet screening.

Another key role of the P-GW is to act as the anchor for mobility between 3GPP and non-3GPP technologies such as WiMAX and 3GPP2 (CDMA 1X and EvDO).

P-GW functions for supporting non-3GPP access (eHRPD) include:

- Mobility anchor for mobility between 3GPP access systems and non-3GPP access systems. This is sometimes referred to as the SAE Anchor function.
- Policy enforcement (gating and rate enforcement)
- Per-user based packet filtering (deep packet inspection)
- Charging support
- Lawful Interception
- UE IP address allocation
- Packet screening
- Transport level packet marking in the downlink;
- Down link rate enforcement based on Aggregate Maximum Bit Rate (AMBR)
- Local Mobility Anchor (LMA) according to draft-ietf-netlmm-proxymip6, if PMIP-based S5 or S8 is used.
- DSMIPv6 Home Agent, as described in draft-ietf-mip6-nemo-v4traversal, if S2c is used.

ESS Features in Release 9.0

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).

Generic L-ESS

In this release, the L-ESS is designed to support simultaneous fetching of any types of files from one or more chassis. That is, it can fetch CDR, EDR, NBR, UDR file, etc.

The current design of L-ESS allows dynamic configuration of source and destination. This further allows multi-threading and multi-processing of the associated hardware components, thereby improving the performance of L-ESS.

Firewall Features in Release 9.0

This section provides information for new features in the Stateful Firewall product in Release 9.0.

Per Subscriber Stateful Firewall Licensing

In previous releases, the Stateful Firewall license was required to enable and configure NAT. In this release, Stateful Firewall and NAT licenses are separated.

The "[600-00-7808] *Stateful Firewall With DPI*" license has been obsoleted.

Stateful Firewall must be enabled and configured using the "[600-00-7571] *Per Subscriber Stateful Firewall 1k sessions*" license. This license enables CLI privileges only for Enhanced Charging Service (ECSv2) and Per Subscriber Stateful Firewall. NAT features cannot be enabled/configured with this license. Some CLI commands that are common to both Stateful Firewall and NAT are available with either Stateful Firewall or NAT license.

For more information, please contact your local sales representative.

GGSN Features in Release 9.0

This section provides information for new features for the GGSN Service in Release 9.0.

GRE Protocol Interface

GRE protocol functionality adds one additional protocol on *ST-series Multimedia Core Platforms* (ST40 or higher) to support mobile users to connect to their enterprise networks through Generic Routing Encapsulation (GRE).

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

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

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

GRE Tunneling consists of three main components:

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

The most simplified form of the deployment scenario is shown in the following figure, in which GGSN has two APNs talking to two corporate networks over GRE tunnels.

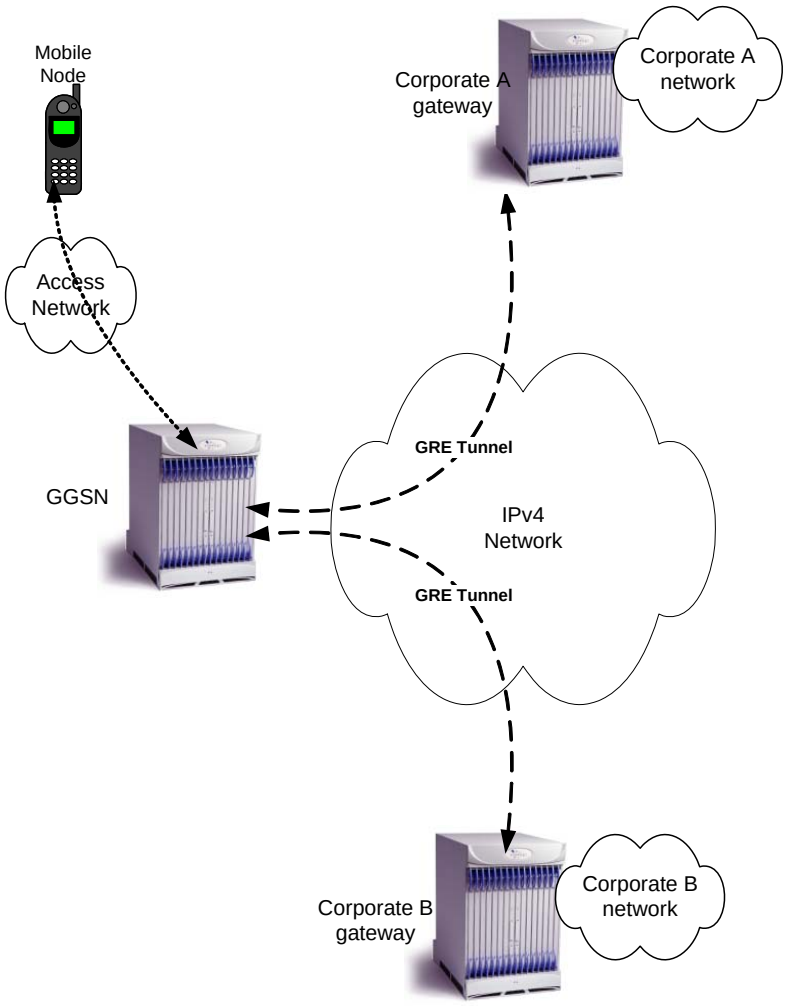

Figure 1-1 GRE Deployment Scenario

Apart from other command configuration addition/modifications in various configuration modes, following new configuration modes were added to Command Line Interface for this feature support:

- OSPF VRF Configuration Mode
- IP VRF Context Configuration Mode
- GRE Tunnel Interface Configuration Mode

This feature requires separate license to enable this for UMTS subscribers.

For more information on functioning and configuration of this interface, refer *GRE Protocol Interface* chapter in *System Enhanced Feature Configuration Guide*.

Overcharging Protection on Loss of Radio Coverage

This solution provides the ability to configure mobile carriers to maximize their network solutions and balancing the requirements to accurately bill their customer.

Consider scenario where a mobile is streaming or downloading very large files from external sources and the mobile goes out of radio coverage. If this download is happening on Background/Interactive traffic class then the GGSN is unaware of such loss of connectivity as SGSN does not perform the Update PDP Context procedure to set QoS to 0kbps (this is done when traffic class is either Streaming or Conversational only). The GGSN continues to forward the downlink packets to SGSN. In the loss of radio coverage, the SGSN will do paging request and find out that the mobile is not responding; SGSN will then drops the packets. In such cases, the G-CDR will have increased counts but S-CDR will not. This means that when operators charge the subscribers based on G-CDR the subscribers may be overcharged. This feature is implemented to avoid the overcharging in such cases.

This implementation is based on Starent-specific private extension to GTP messages and/or any co-relation of G-CDRs and S-CDRs. It also does not modify any RANAP messages.

This feature requires separate license to enable this for UMTS subscribers.

For more information of this feature, refer *Subscriber Overcharging Protection* chapter in *System Enhanced Feature Configuration Guide*.

GSS Features in Release 9.0

This section provides information for new GSS features for Release 9.0

Multiple Instance GSS

Release 9.0 enables support for multiple data streams from one server or a single cluster setup to utilize multiple instances of GSS with a single installation and multiple databases.

In a cluster setup, there is only one installation per node. During installation, GSS is installed at a fixed location (*/opt/gss_global* directory). The initial GSS installation does not create any GSS instance. Once GSS is installed on both the nodes, the */opt/gss_global/make_gss_instance* script utility creates instances as an when needed and validates the conflicting ports/username across the instances.

For all instances on the node, only one set of binaries and scripts are used. Each instance will have its own configuration file, log directory, tools directory and separate PostgreSQL database. The alarms and events generated by each instance are sent to its corresponding chassis. Individual GSS instance can also be stopped, started or switched over. Upgrade is smooth and will involve minimum down time as possible.

Each GSS instance can be uninstalled separately and will not have any impact on the other instances. Global installation can be only uninstalled if there are no instances configured or running on the system.

The advantages of this feature include:

- Only one installation required for multiple instances
- One binary used across all the instances on the node
- Upgrading one set of binaries would upgrade all the instances
- In cluster mode resource groups, instances can be balanced across the nodes

For more information on the installation, uninstallation and upgrade procedures for multiple GSS instances, refer to *Multiple Instances of GSS* section in *GSS Installation Management* chapter of *GSS Installation and Administration Guide*.

Monitoring of Disk Partitions

This feature enables support for disk monitoring of shared postgres and gss installation disk partition along with GSS data files disk partition. This feature is supported only for single instance GSS, and for GSS in cluster mode.

This feature can be enabled after installation by configuring specific parameters in the gss configuration file. For information on configuring the parameters, refer to the *Modifying a GSS Configuration* section in the *GTPP Storage Server Administration* chapter of *GSS Installation and Administration Guide*.

IMPORTANT

This feature does not support backward compatibility and hence GSN build should always match with GSS build.

HA Features in Release 9.0

This section provides information for new features in the Home Agent product in Release 9.0.

None for this release.

inPilot Features in Release 9.0

This section provides information for new inPilot features in Release 9.0.

Bulkstat and KPI Reports

The Bulkstat report provides details of the processed bulk statistics from any application (PDSN, GGSN, SGSN, and so on) on the managed nodes in a timely manner. Users need to be assigned to the Region levels so that when a user logs in to the inPilot Server, the data can be viewed for all nodes under the parent node. Only the Admin users are assigned to the top of the tree (root node or NOC node) and have access to the whole network data. The Bulkstat Report can be viewed for the desired bulkstats by selecting the **BULKSTAT** tab.

The KPI report provides details of the KPIs for each selected schema. The KPI Report can be viewed for the desired KPIs by selecting the **KPI** tab.

Exporting Reports to PDF Format

The inPilot application now supports exporting reports to PDF file format.

To export a report to PDF format, in the **HOME** and **DPI REPORTS** tabs of the inPilot GUI, click the **Export to PDF** button. The PDF file is displayed in a new window and can be saved for future reference. If there is no data available for a report, the **Export to PDF** button is disabled.

GUI/Console based Installation

The inPilot application and its components can be installed and uninstalled using one of the following two methods.

- Using script-based installer
- Using GUI/console-based installer

Log File Path

After inPilot upgrade to newer versions, the log files are generated at */starbi/logs/* directory as against the */starbi/server/logs* directory in previous releases.

RAT Classification Report

RAT Classification Report can be viewed under **Available Reports** in the **HOME** tab.

RAT Type reports are generated only if a RAT-type variable is available in EDRs. The RAT related parameters are applicable only for a GGSN call.

If a RAT-type variable is not available, then all the traffic is displayed as Unclassified RAT Type in RAT Type reports. This is the case for a PDSN call.

Supported File System

inPilot now recommends the ZFS file system with two ZFS pools for Sun Microsystems Netra™ T5220 and Sun Microsystems Netra™ X4450 servers. The inPilot installation procedure also includes a checkpoint for ZFS when the user performs installation on a non-ZFS partition path.

Voice Call Duration Reports

The TopN VCD Subscribers report displays the top N subscribers based on their voice usage (voice duration) for Yahoo, MSN and Skype voice protocols. The summary report displays the voice summary (voice duration) for VoIP category.

TopN VCD Subscribers Report can be viewed under **Available Reports** in the **HOME** tab.

For more information on the above mentioned features, refer to *inPilot Installation and Administration Guide* and *inPilot Online Help*.

IP Services Gateway Features in Release 9.0

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

None for this release.

LTE/SAE Features in Release 9.0

This section contains information on new 9.0 features that pertain to the PDN Gateway (P-GW), the Mobility Management Entity (MME) and the Serving Gateway (S-GW) supporting LTE network services.

New P-GW Features

The P-GW is new in Release 9.0.

The P-GW terminates the SGi interface towards the Packet Data Network (PDN). If a UE is accessing multiple PDNs, there may be more than one P-GW for that UE. The P-GW provides connectivity to the UE to external packet data networks by being the point of exit and entry of traffic for the UE. A UE may have simultaneous connectivity with more than one P-GW for accessing multiple PDNs. The P-GW performs policy enforcement, packet filtering for each user, charging support, lawful interception and packet screening.

The P-GW provides the following basic functions:

- Terminates the interface towards the PDN (SGi)
- PGW functions for GTP-based S5/S8 include:
  - per-user packet filtering (e.g.deep packet inspection)
  - lawful intercept
  - UE IP address allocation
  - UL and DL service level charging, gating control, and service level rate enforcement
  - DL rate enforcement based on AMBR (Aggregate Max Bit Rate) and based on the accumulated MBRs of the aggregate of SDFs with the same GBR QCI
  - DHCPv4 and DHCPv6 functions (client, relay and server)

New MME Features

The MME is new in Release 9.0.

The MME resides in the control plane and manages states (attach, detach, idle, RAN mobility), authentication, paging, mobility with 3GPP 2G/3G nodes (SGSN), roaming, and other bearer management functions. The MME is the key control-node for the LTE access-network. The MME provides the following basic functions:

- NAS
  - signalling
  - signalling security
- UE access in ECM-IDLE state (including control and execution of paging retransmission)
- Tracking Area (TA) list management
- P-GW and S-GW selection
- MME selection for handovers with MME change

- SGSN selection for handovers to 2G or 3G 3GPP access networks
- Terminates interface to HSS (S6a)
- Authentication
- Bearer management functions including dedicated bearer establishment
- HRPD access node (terminating S101 reference point) selection for handovers to HRPD
- Transparent transfer of HRPD signalling messages and transfer of status information between E-UTRAN and HRPD access, as specified in the pre-registration and handover flows

New S-GW Features

The Serving Gateway routes and forwards data packets from the UE and acts as the mobility anchor during inter-eNodeB handovers. Signals controlling the data traffic are received on the S-GW from the MME which determines the S-GW that will best serve the UE for the session. Every UE accessing the EPC is associated with a single S-GW.

For each UE associated with the EPS, there is a single S-GW at any given time providing the following basic functions:

- Terminates the interface towards E-UTRAN (S1-U)
- Functions for the GTP-based S5/S8 include:
  - local mobility anchor point for inter-eNodeB handover
  - mobility anchoring for inter-3GPP mobility (terminating S4 and relaying the traffic between 2G/3G system and P-GW)
  - ECM-IDLE mode downlink packet buffering and initiation of network triggered service request procedure
  - lawful intercept
  - packet routing and forwarding
  - transport level packet marking in the uplink and the downlink (e.g. setting the DiffServ Code Point)
  - Accounting

NAT Features in Release 9.0

This section contains information for new features in the Network Address Translation (NAT) product in Release 9.0.

NAT Licensing

In previous releases, the Stateful Firewall license was required to enable and configure NAT. In this release, Stateful Firewall and NAT licenses are separated.

The "[600-00-7804] *NAT/PAT Without DPI*" license has been obsoleted.

NAT must now be enabled and configured using the "[600-00-7805] *NAT/PAT With DPI*" license. This license enables CLI privileges only for Enhanced Charging Service (ECSv2) and NAT/PAT with DPI. Stateful Firewall features cannot be enabled/configured with this license. Some CLI commands that are common to both NAT and Stateful Firewall will be available with either NAT or Stateful Firewall license.

For more information, please contact your local sales representative.

PDG/TTG Features in Release 9.0

The PDG/TTG is a new product in Release 9.0. The PDG/TTG enables mobile operators to provide Fixed Mobile Convergence (FMC) services to subscribers with dual-mode handsets and dual-mode access cards via WiFi access points. The PDG/TTG makes it possible for operators to provide secure access to the operator's 3GPP network from a non-secure network, reduce the load on the macro wireless network, enhance in-building wireless coverage, and make use of existing backhaul infrastructure to reduce the cost of carrying wireless calls.

This PDG/TTG software release provides TTG functionality. The TTG is a network element that enables 3GPP PDG functionality for existing GGSN deployments. The TTG and the subset of existing GGSN functions work together to provide PDG functionality to the subscriber UEs in the WLAN.

The PDG/TTG is a licensed product. For information about PDG/TTG licenses, contact your Starent representative.

IMPORTANT

This PDG/TTG software release provides TTG functionality only. PDG functionality is not supported in this release.

The TTG features and functions in this release include:

- PDG service
- TTG mode
- IKEv2 and IP Security (IPSec) encryption
- Multiple digital certificate selection based on APN
- Subscriber traffic policing for IPSec access
- DSCP marking for IPSec access
- WLAN access control
- RADIUS and Diameter support
- EAP fast re-authentication
- Pseudonym NAI support
- Multiple APN support for IPSec access
- Congestion control
- Bulk statistics
- Threshold crossing alerts (TCAs)

For more information about TTG features and functions, see the *PDG/TTG Administration Guide*.

PDIF Features in Release 9.0

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

Multiple Traffic Selectors

The PDIF can be configured with multiple IPsec traffic classes, each containing up to 128 traffic selectors, which are used during traffic selector negotiation with UEs. Multiple traffic selectors allow the PDIF to direct outbound traffic to selected IP addresses based on the following protocols: IP, TCP, UDP, and ICMP. The PDIF can also direct TCP and UDP traffic to selected IP addresses and port ranges.

IMPORTANT

In this software release, the PDIF supports IPv4 traffic selectors only.

Selective Diameter Profile Update Request Control

For mobile IP calls, the Selective Diameter Profile Update Request Control feature allows WiFi data-only sessions to co-exist with VoIP sessions on the PDIF platform.

When the PDIF is accessed by voice-enabled devices, it needs to interact with the HSS in order for a subscriber session to access the IP core network. When the PDIF is accessed by data-only devices, there is no need to interact with the HSS.

This feature is used to identify which subscriber sessions need to have the PDIF and the HSS exchange Diameter Profile Update Request (PUR) and Profile Update Answer (PUA) messages, and allows the PDIF to handle the call setup for a data-only client without having to interact with the HSS.

Selective PUR profiles on the AAA server are mapped to subscribers during AAA authentication via the Radius vendor-specific attribute (VSA) FMC-Type. FMC-Type has these possible values: voice or data. When the AAA server sets the FMC-Type value to voice, the PDIF and the HSS exchange PUR and PUA messages. When the AAA server sets the FMC-Type value to data, the PDIF and the HSS do not exchange PUR and PUA messages.

For more information about PDIF features and functions, see the *Packet Data Interworking Function Administration Guide*.

PDSN Features in Release 9.0

This section provides information for new features in the Packet Data Serving Node in Release 9.0.

None for this release.

Peer-to-Peer Features in Release 9.0

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

Dynamic P2P Signature Updates

P2P traffic detection is tricky because most of the P2P protocol details are proprietary, and the protocol characteristics change frequently. As these P2P standards are proprietary, there is a tight coupling between the peers too (all the peers need to understand the protocols). Since P2P detection depends heavily on the known traffic characteristics the detection can suffer if the P2P protocol changes, if some existing traffic characteristics were not known (new use case scenarios), if one P2P traffic characteristic matches with another P2P traffic (false positives), and if there are flaws (bugs) in the detection logic. Whenever such degradation in P2P detection logic is identified, the P2P detection logic must be enhanced to improve the detection accuracy.

In the earlier releases, the P2P detection logic was part of the ST-chassis software load (ST16/ST40 software), to continue to detect new traffic patterns based on the changing traffic characteristics, operators needed to upgrade the complete software with the updated detection logic.

This release supports dynamic upgrades of the P2P detection logic (signatures) alone on an active ST16/ST40 without warranting a full software upgrade, and hence without a software restart or reboot. This is implemented through signature files.

IMPORTANT

This release supports dynamic signature upgrades for the following P2P protocols: Bittorrent, DirectConnect, eDonkey, Gnutella, Skype, Yahoo

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

P2P Protocols Detection Support

With release 9.0, the system supports detection of the following P2P protocols:

- GTalk
  - Voice
  - Non-voice
- ooVoo

With release 9.0, the system supports enhanced detection accuracy, for charging purposes, for the following P2P protocols:

- GTalk
  - Voice
  - Non-voice
- Mute

- ooVoo
- Oscar:
  - Voice
  - Non-voice
- Pando
- QQlive
- SopCast

SCM Features in Release 9.0

This section provides information for new features in Release 9.0 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*.

IPv4-IPv6 Interworking

Benefits

This feature allows the P-CSCF to provide IPv4-IPv6 interworking in the following scenarios:

- When UEs are IPv6-only and the IMS core network is IPv4-only
- When UEs are IPv4-only and the IMS core network is IPv6-only

In addition, IPv4-IPv6 interworking helps an IPv4 IMS network transition to an all-IPv6 IMS network.

The following interworking requirements are currently supported:

- IPv4 TCP and IPv6 TCP
- Transport switching allowed based on size for both v4 and v6 network
- UDP fragmentation allowed for both v4 and v6 networks
- P-CSCF supports Mw and Gm interfaces on both v4 and v6
- KPIs for Mw and Gm interfaces are supported on both v4 and v6
- DNS supported for v4 and v6 networks
- Interworking supported for IM and presence
- Both v4 and v6 handsets are supported simultaneously on the same P-CSCF node

Description

P-CSCF will provide IPv4-IPv6 interworking functionality between IPv6-only UEs and IPv4-only core network elements (I/S-CSCF) by acting as a dual stack. To achieve the dual-stack behavior, P-CSCF will be configured in two services with the first service (V6-SVC) listening on an IPv6 address and the second service (V4-SVC) listening on an IPv4 address. SIP messages coming from IPv6 UEs will come to V6-SVC and will be forwarded to the IPv4 core network through V4-SVC. Similarly, messages from the IPv4 core network come to V4-SVC and will be forwarded to IPv6 UEs via V6-SVC. P-CSCF also provides interworking functionality between IPV4-only UEs and IPv6-only core network elements.

To identify the need for v4-v6 interworking for a new incoming IPv6 REGISTER arriving at V6-SVC, a route lookup is performed based on the request-uri, first in V4-SVC context and then in V6-SVC context if the first lookup does not return any matching route entry. If a matching IPv4 next-hop route entry is found, then this indicates that interworking needs to be done. If no route entry is found, then a DNS query on request-uri domain is done for both A and AAAA type records. If DNS response yields only an IPv4 address, then this is also the case for performing v4-v6 interworking.

Headers (such as Via, Path, etc.) are automatically set to IPv4 bind address of P-CSCF V4-SVC. Remaining headers will be not be altered and sent as is toward the S-CSCF. The IPv4 address in a Path header received from S-CSCF in 200Ok of REGISTER will be replaced with V6-SVC's IPv6 address before forwarding to UE.

P-CSCF handling different v4-v6 interworking scenarios is shown below.

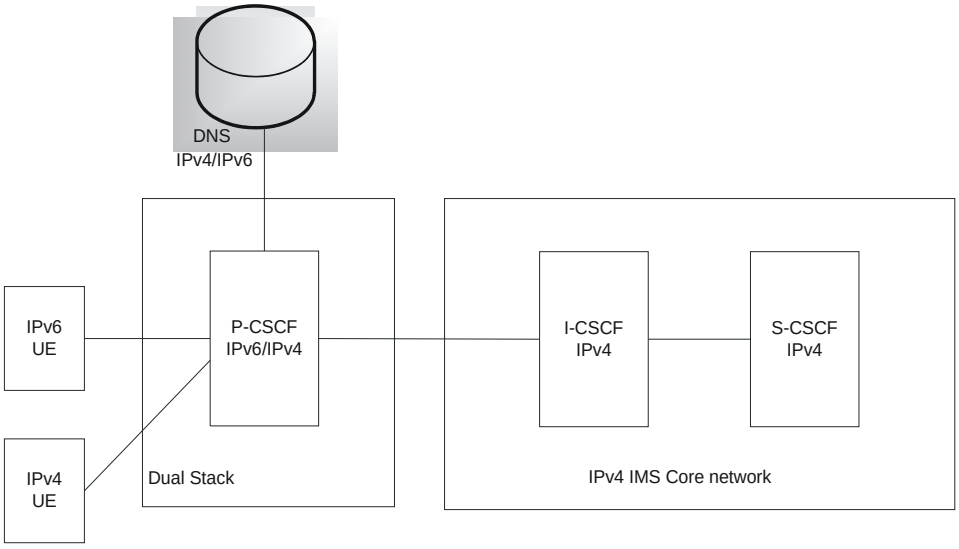

Figure 1-2 Interworking Between IPv6 UE and IPv4 IMS Core Network

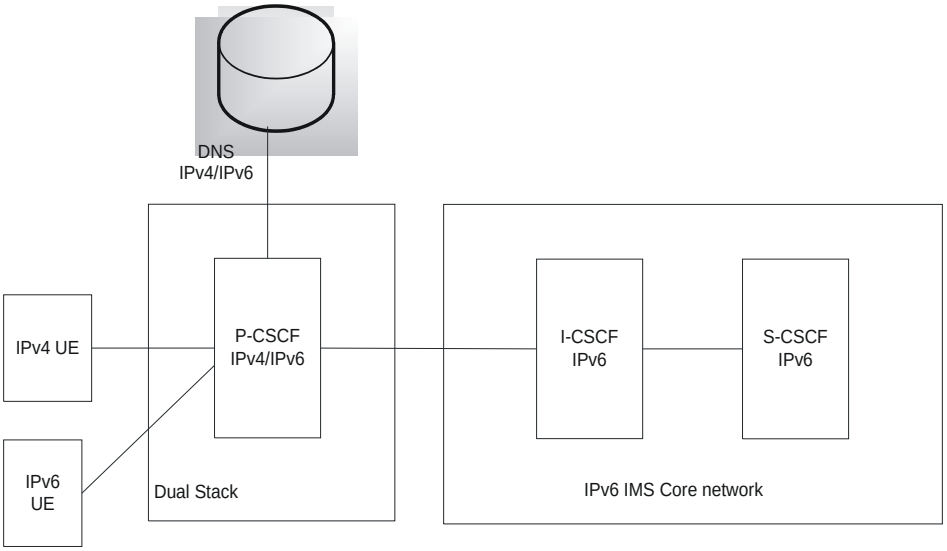

Figure 1-3 Interworking Between IPv4 UE and IPv6 IMS Core Network

SGSN Features in Release 9.0

This section provides information for new features in Release 9.0 for the Serving GPRS Support Node (SGSN). Additional information on these features can be found in the *SGSN Overview* section of the *Product Overview*, in the *SGSN Administration Guide*, and in the *CLI Reference Guide*.

Configurable Gf IMEI Check Event Timer

PR 127561; ST16 PR 127561

The lower boundary for the 1-in-N IMEI check timer has been changed to 1 second. Now the configurable timeout range is 1 to 30 seconds, with a default of 15 seconds.

Previously, the configurable timeout range was 15 to 30 seconds per the 3GPP specification.

For more information, refer to the *MAP Service Configuration Mode* chapter of the *Command Line Interface Reference*.

Default APN

Operators can configure a “default APN” for subscribers not provisioned in the HLR. This feature is available in releases 8.1 and higher.

The Default APN feature will be used in error situations when the SGSN cannot select a valid APN via the normal APN selection process. Within an operator policy, a default APN can be configured for the SGSN to: override a requested APN when the HLR does not have the requested APN in the subscription profile. provide a viable APN if APN selection fails because there was no “requested APN” and wildcard subscription was not an option.

In either of these instances, the SGSN can provide the default APN as an alternate behavior to ensure that PDP context activation is successful.

Refer to the *SGSN Operator Policy Configuration Mode* in the *Command Line Interface Reference* for the command to configure this feature.

Disable Signaling Indication IE in RANAP messages

In accordance with RANAP standards, the Signaling Indication IE is only included in RANAP messages RANAP (RAB Assignment Request and/or the Relocation Request messages) when the traffic class is “interactive”.

The Command Line Interface (CLI) has been modified to enable the operator to control whether the IE is included if *both* of the following conditions are met:

1.when the traffic class is “interactive”.

2.Signaling Indication IE is included in the current QoS and the value is optimized (value of “1”).

New CLI commands have been added to the RNC configuration mode to govern the inclusion of the Signaling Indication IE in RANAP messages. Refer to the *Command Line Interface Reference* for information on enabling/disabling this feature.

Limiting Iu Connections in RANAP Messages

A new command has been created to enable the operator to further control message length by configuring the number of **`IuConIDs`** sent in each SGSN Init Reset Resource message.

This change will have no impact on current or future configurations as the previously coded system value was 250.

Refer to the *RNC Configuration Mode* chapter of the *Command Line Interface Reference* for additional information.

Limits / Engineering Rules

The following limits for release 9.0 have been modified in the Engineer Rules appendix of the *SGSN Administration Guide*.

- 2G Interface Rules:
  - Maximum number of NSEs has increased from 256 to 512
  - Maximum number of NSEs controlling the same RA has increased from 64 to 128
- Connection Rules:
  - Max # of logically connected GGSNs per Gn/Gp intf increased from 20,000 to “no limit”
  - Max # of packets buffered -- rules have been clarified:
    - Minimum of 2KB/subscriber.
    - Maximum of 10KB/subscriber -- if buffers are available in the shared pool*.
    (*SGSN provides a buffer pool of 10M per session manager - buffer to be shared by all subscribers “belonging” to that session manager.)
- SIGTRAN: Max number of peer servers per SS7RD increased from 144 to 256.

Correction:

- Max# of RNCs per 3G intf: corrected from 1024 to 256.

Lawful Intercept

The SGSN now supports Phase 1 LI Buffering. For details, please contact your customer sales or support representative.

Local QoS Capping

The operator can configure a cap or limit for the QoS bit rate.

The SGSN can now be configured to cap the QoS bit rate parameter when the subscribed QoS provided by the HLR is lower than the locally configured value.

Depending upon the keywords included in the command, the SGSN can: take the QoS parameter configuration from the HLR configuration. take the QoS parameter configuration from the local settings for use in the APN policy. during session establishment, apply the lower of either the HLR subscription or the locally configured values.

Refer to the *SGSN APN Policy Configuration Mode* chapter of the *Command Line Interface Reference* for the qos command.

Multiple PLMN Support

With this feature, the 3G SGSN now supports more than one PLMN ID per SGSN. Multiple PLMN support facilitates MS handover from one PLMN to another PLMN.

Multiple PLMN support also means an operator can 'hire out' their infrastructure to other operators who may wish to use their own PLMN IDs. As well, multiple PLMN support enables an operator to assign more than one PLMN ID to a cell-site or an operator can assign each cell-site a single PLMN ID in a multi-cell network (typically, there are no more than 3 or 4 PLMN IDs in a single network).

This feature is enabled by configuring, within a single context, multiple instances of either an IuPS service for a single 3G SGSN service. Each IuPS service is configured with a unique PLMN ID. Each of the SGSN services must use the same MAP, SGTPU and GS services so these only need to be defined one-time per context.

Overcharging Protection

Overcharging Protection enables the SGSN to avoid overcharging the subscriber if/when a loss of radio coverage (LORC) occurs.

When a mobile is streaming or downloading files from external sources (via background or interactive traffic class) and the mobile goes out of radio coverage, the GGSN is unaware of such loss of connectivity and continues to forward the downlink packets to the SGSN.

To accommodate such situations, the SGSN can be configured to set a proprietary private IE extension to set the QoS to 0kbps upon a loss of radio coverage occurs. This setting notifies the GGSN of the LORC to prevent overcharging.

Refer to the *SGSN APN Policy Configuration Mode* chapter of the *Command Line Interface Reference* for the command to configure the GTPC private extension and refer to the *IuPS Service Configuration Mode* chapter of the *Command Line Interface Reference* to configure the LORC Cause IE.

PSC2 - Packet Services Card 2

The SGSN now supports the Packet Services Card 2 (PSC2), the next-generation packet forwarding card for the ST40. The PSC2 provides increased aggregate throughput and performance, and a higher number of subscriber sessions. For more information about this card, refer to the "SGSN Overview" in the *SGSN Administration Guide* and the *ST40 Hardware Installation and Administration Guide*.

Suppression of Paging Cause IE in Paging Request

The CLI has been modified to allow the operator to configure suppression of the Paging Cause IE in a Paging Request. As well, the operator has been given the ability to configure the cause value for various paging sources.

For details, refer to the **ranap** command in the *RNC Configuration Mode* chapter of the *Command Line Interface Reference*.

Tracking Usage of GPRS Encryption Algorithm

Usage of the GPRS encryption algorithm (GEA) significantly affects the SGSN processing capacity depending upon the GEAx level used - GEA1, GEA2, or GEA3.

Operators could use a mechanism that would enable them to identify the percentages of their customer base that are using the various GEA encryption algorithms. The same tool would also track the migration trend from GEA2 to GEA3 and allow an operator to forecast the need for additional SGSN capacity to exceed.

Enhanced counters should display the absolute number of attached subscribers using each of the GEA algorithms.

Counters have been added to the output of the **show sub gprs-only summary** CLI command to track:

- the number of subscribers capable of GEA0-GEO3, and
- the number of subscribers with negotiated GEAx levels.

New counters display the number of subscribers whose MS network capability supports GEA0/GEA1/GEA2/GEA3. Similarly, the new counters under "Negotiated" indicate the number of subscribers who have negotiated with the SGSN to use a specific encryption algorithm according to the ciphering priority configuration and the network capability.

Sample Output:

```
[local]bngnc3# show sub gprs-only sum

Total Subscribers           : 2         Total Ready Subscribers      : 0
Total Detached Subscribers  : 1         Total Standby Subscribers    : 1
Total Suspended Subscribers  : 0
Total subscribers with encryption algorithm
                  Capability :                              Negotiated :
                    GEA0     : 1                             GEA0     : 1
                    GEA1     : 0                             GEA1     : 0
                    GEA2     : 0                             GEA2     : 0
```

```
                      GEA3     : 1                              GEA3     : 0
Total Active Subscribers       : 0        Total PDP contexts             : 0
pdp-type-ipv4                  : 0        pdp-type-ppp                   : 0
pdp-type-ipv6                  : 0
.
.
```

XGLC - 10 Gigabit Ethernet Line Card

The 10 Gigabit Ethernet Line Card is commonly referred to as the XGLC. The XGLC supports higher speed connections to packet core equipment, increases effective throughput between the ST40 and the packet core network, and reduces the number of physical ports needed on the ST40. For more information about this card, refer to the “SGSN Overview” in the *SGSN Administration Guide* and the *ST40 Hardware Installation and Administration Guide*.

Web Element Manager Features in Release 9.0

This section provides information for new features for the Web Element Manager application in Release 9.0.

None for this release.

CHAPTER 2
FAULT MANAGEMENT

This section contains additions and changes made to the fault management features available in Release 9.0.

SNMP MIB Objects in Release 9.0

This section lists the MIB objects and alarms new / modified in Release 9.0.

New Objects

- starASNPCServiceStart
- starPDGServiceStart
- starPDGServiceStop
- starDiameterIpv6PeerDown
- starDiameterIpv6PeerUp
- starIPMSServerUnreachable
- starIPMSServerReachable
- starCertShortLifetime
- starCertExpired
- starCertValid
- starFTPPushFail
- starFTPServSwitch
- starSDHSectionDown
- starSessTtlOctForwardedGB
- starPortRxDiscards
- starPortTxDiscards
- starPortRxErrors
- starPortTxErrors
- starPDGSysStatus
- starPDGSysNumService
- starPDGSysSessCurrent
- starPDGSysSessCurrActive
- starPDGSysSessCurrDormant
- starPDGSysSessTtlSetup
- starPDGSysChildSACurrent
- starPDGTable
- starPDGEntry
- starPDGSvcID
- starPDGVpnID
- starPDGVpnName
- starPDGServName
- starPDGStatus
- starPDGSessCurrent

- starPDGSessRemain
- starPDGSessCurrentActive
- starPDGSessCurrentDormant
- starPDGSessCurrentIpv6Dormant
- starPDGSessCurrentIpv4Active
- starPDGSessCurrentIpv4Dormant
- starPDGBindIpAddress
- starPDGBindIpPort
- starPDGBindSlot
- starThreshPHSGWSessTimeout
- starThreshClearPHSGWSessTimeout
- starThreshPHSGWSessSetupTimeout
- starThreshClearPHSGWSessSetupTimeout
- starThreshPHSGWAuthFail
- starThreshClearPHSGWAuthFail
- starThreshPHSGWMaxEAPRetry
- starThreshClearPHSGWMaxEAPRetry
- starThreshPHSGWNWEntryDenial
- starThreshClearPHSGWNWEntryDenial
- starThreshPHSGWHandoffDenial
- starThreshMeasuredInt
- starThreshPHSPCSessSetupTimeout
- starThreshClearPHSPCSessSetupTimeout
- starThreshPHSPCSleepModeTimeout
- starThreshClearPHSPCSleepModeTimeout
- starThreshPHSPCSmEntryDenial
- starThreshClearPHSPCSmEntryDenial
- starPHSGWServiceStart
- starPHSGWServiceStop
- starPHSPCServiceStart
- starPHSPCServiceStop
- starDynPkgLoadError
- starDynPkgLoadErrorClear
- starDynPkgUpgradeError
- starDynPkgUpgradeErrorClear
- starThreshGPRSSessions
- starThreshClearGPRSSessions
- starThreshPerServiceGPRSSessions

- starThreshClearPerServiceGPRSSessions
- starThreshGPRSPdpSessions
- starThreshClearGPRSPdpSessions
- starThreshPerServiceGPRSPdpSessions
- starThreshClearPerServiceGPRSPdpSessions
- starEGTPInterfaceType
- starEGTPSelfPort
- starEGTPSelfAddr
- starEGTPPeerPort
- starEGTPPeerAddr
- starEGTPPeerOldRstCnt
- starEGTPPeerNewRstCnt
- starEGTPPeerSessCnt
- starEGTPFailureReason
- starServiceLossPTACsClear
- starServiceLossLCClear
- starOSPFv3NeighborDown
- starOSPFv3NeighborFull
- starServiceLossSPIOClear
- starCscfSessCongestionResourceType
- starSmgrId
- starFNGSysStatus
- starFNGSysNumService
- starFNGSysSessCurrent
- starFNGSysSessCurrActive
- starFNGSysSessCurrDormant
- starFNGSysSessTtlSetup
- starFNGSysChildSACurrent
- starFNGTable
- starFNGEntry
- starFNGSvcID
- starFNGVpnID
- starFNGVpnName
- starFNGServName
- starFNGStatus
- starFNGSessCurrent
- starFNGSessRemain
- starFNGSessCurrentActive

- starFNGSessCurrentDormant
- starFNGSessCurrentIpv6Active
- starFNGSessCurrentIpv6Dormant
- starFNGSessCurrentIpv4Active
- starFNGSessCurrentIpv4Dormant
- starFNGBindIpAddress
- starFNGBindIpPort
- starFNGBindSlot
- starFNGBindPort
- starCscfSessResourceCongestion
- starCscfSessResourceCongestionClear
- starCSCFPeerServerUnavailable
- starCSCFPeerServerOutofService
- starCSCFPeerServerInService
- starThreshCSCFSvcRegPerInterval
- starThreshClearCSCFSvcRegPerInterval
- starThreshCSCFSvcTotalActiveReg
- starThreshClearCSCFSvcTotalActiveReg
- starThreshCSCFSvcCallsPerInterval
- starThreshClearCSCFSvcCallsPerInterval
- starThreshCSCFSvcTotalActiveCalls
- starThreshClearCSCFSvcTotalActiveCalls
- starThreshCSCFSvcTotalCallFailure
- starThreshClearCSCFSvcTotalCallFailure
- starThreshCSCFSvcErrorNoResource
- starThreshClearCSCFSvcErrorNoResource
- starThreshCSCFSvcErrorTcp
- starThreshClearCSCFSvcErrorTcp
- starThreshCSCFSvcErrorPresence
- starThreshClearCSCFSvcErrorPresence
- starThreshCSCFSvcErrorRegAuth
- starThreshClearCSCFSvcErrorRegAuth
- starThreshSGWSessions
- starThreshClearSGWSessions
- starThreshPGWSessions
- starThreshClearPGWSessions
- starThreshLMASessions
- starThreshClearLMASessions

- starThreshMAGSessions
- starThreshClearMAGSessions
- starThreshPHSGWEAPOLAuthFailure
- starThreshClearPHSGWEAPOLAuthFailure
- starThreshPHSGWMaxEAPOLRetry
- starThreshClearPHSGWMaxEAPOLRetry
- starASNPCServiceStart
- starASNPCServiceStop
- starDiameterIpv6PeerDown
- starDiameterIpv6PeerUp
- starIPMSServerUnreachable
- starIPMSServerReachable
- starCertShortLifetime
- starPGWServiceStart
- starPGWServiceStop
- starSGWServiceStart
- starSGWServiceStop
- starEGTPServiceStart
- starEGTPServiceStop
- starLMAServiceStart
- starLMAServiceStop
- starMAGServiceStart
- starMAGServiceStop
- starMMEServiceStart
- starMMEServiceStop
- starHSGWServiceStart
- starHSGWServiceStop
- starCPUBusyClear
- starCPUMemoryLowClear
- starFNGServiceStart
- starFNGServiceStop
- starManagerRestart
- starConfigurationUpdate
- starEgtpcPathFailure
- starEgtpcPathFailureClear
- starEgtpuPathFailure
- starEgtpuPathFailureClear
- starThreshFNGCurrSess

- starThreshClearFNGCurrSess
- starThreshFNGCurrActSess
- starThreshClearFNGCurrActSess
- starThreshBGPRoutes
- starThreshClearBGPRoutes
- starThreshNAPTPortChunks
- starThreshHSGWSessions

Modified Objects

- starCongestionResourceType
- starThreshLicense

Obsoleted Objects

- starCardSWFailed
- starCardFailureLEDOn

Deleted Objects

None for this release.

New Alarms

None for this release.

Modified Alarms

- starSDHSectionDown
- starSDHSectionUp
- starSDHPathHopDown
- starSDHPathHopUp
- starSDHLopDown
- starSDHLopUp
- starSDHE1TribUp
- starSDHFractE1LMIDown
- starSDHFractE1LMIUp
- starGPRSServiceStart
- starGPRSServiceStop
- starGPRSNseUp
- starGPRSNsvcDown

- starGPRSNsvcUp
- starGPRSBvcDown
- starGPRSBvcUp
- starCongestionResourceType

Obsoleted Alarms

None for this release.

Deleted Alarms

None for this release.

Web Element Manager Path

Select Configuration | SNMP Configuration.

Content Filtering MIB Objects for Release 9.0

This section lists the Content Filtering MIB objects and alarms new/modified in Release 9.0.

New Objects

None for this release.

Modified Objects

None for this release.

Obsoleted Objects

None for this release.

Deleted Objects

None for this release.

New Alarms

None for this release.

Modified Alarms

None for this release.

Obsoleted Alarms

None for this release.

Deleted Alarms

None for this release.

Web Element Manager Path

Select Configuration | SNMP Configuration.

ESS MIB Objects for Release 9.0

This section lists the new and modified MIB objects and alarms for Local-External Storage Server (L-ESS) in Release 9.0.

New Objects

None for this release.

Modified Objects

None for this release.

Obsoleted Objects

None for this release.

Deleted Objects

None for this release.

New Alarms

None for this release.

Modified Alarms

None for this release.

Obsoleted Alarms

None for this release.

Deleted Alarms

None for this release.

Intelligent Packet Monitoring Systems (IPMS) MIB in Release 9.0

This section lists the new and modified MIB objects and alarms for IPMS in Release 9.0.

New Objects

None for this release.

Modified Objects

None for this release.

Obsoleted Objects

None for this release.

Deleted Objects

None for this release.

New Alarms

None for this release.

Modified Alarms

None for this release.

Obsoleted Alarms

None for this release.

Deleted Alarms

None for this release.

Web Element Manager Path

Select Configuration | SNMP Configuration.

Web Element Manager Enhancements in Release 9.0

This section contains new and modified MIB objects and alarms for Web Element Manager. in Release 9.0.

New Objects

- starEmsConfigBackupFtpFailed
- starEmsConfigBackupFtpSuccess

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 9.0. Topics covered in this chapter are:

- *New Configuration Commands*
- *Modified Configuration Commands*
- *Obsoleted Commands*
- *GTPP Storage Server (GSS)*
- *Web Element Manager Changes*

New Configuration Commands

This section contains configuration commands that are new in Release 9.0. New commands in this version are divided into the following sections:

- *Common Commands - New in Release 9.0*
- *ASN GW Commands - New in Release 9.0*
- *Content Filtering Commands - New in Release 9.0*
- *ECS Commands - New in Release 9.0*
- *Firewall Commands - New in Release 9.0*
- *GGSN Commands - New in Release 9.0*
- *HA Commands - New in Release 9.0*
- *NAT Commands - New in Release 9.0*
- *PDIF Commands - New in Release 9.0*
- *PDSN Commands - New in Release 9.0*
- *Peer-to-Peer - New in Release 9.0*
- *Session Control Manager Commands - New in Release 9.0*
- *SGSN Commands - New in Release 9.0*

Common Commands - New in Release 9.0

This section provides information on new commands that are common to products in Release 9.0.

apn-name-to-be-included

This command configures the APN name to be included in CCR Gx messages.

CLI (Policy Control Configuration Mode)

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

Web Element Manager Path

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

cdr-multi-mode

This command enables multiple instances of CDRMOD.

CLI (Global Configuration Mode)

```
[ default ] cdr-multi-mode
```

Web Element Manager Path

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

ip vrf

New command added to create new configuration mode named IP VRF Context Configuration Mode to configure the parameters for GRE tunnel interface support. This command configures Virtual Routing and Forwarding (VRF) parameters and also creates IP VRF Context instance for GRE tunnel interface configuration. For more information, refer *IP VRF Context Configuration Mode Commands* chapter in *Command Line Interface Reference*.

CLI (Context Configuration Mode)

ip vrf *vrf_name*
no ip vrf

Web Element Manager Path

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

ip vrf

New command added to create new configuration mode named OSPF VRF Configuration Mode to configure the virtual routing and forwarding (VRF) context instances for OSPF routing protocol. This mode includes commands that configure VRF instance for OSPF routing parameters. For more information, refer *OSPF VRF Context Configuration Mode Commands* chapter in *Command Line Interface Reference*.

CLI (OSPF Configuration Mode)

ip vrf *vrf_name*
no ip vrf

Web Element Manager Path

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

ip vrf forwarding

New command added to configure the parameters for GRE tunnel interface support. This command configures the IP VRF forwarding and associates preconfigured VRF context with the current interface for GRE tunnel interface configuration.

CLI (Tunnel Interface Configuration Mode)

ip vrf forwarding *vrf_name*
no ip vrf forwarding

Web Element Manager Path

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

radius ip vrf

New command added to configure the parameters for GRE tunnel interface support. This command associates the Virtual Routing and Forwarding (VRF) Context instance for GRE tunnel interface configuration with specific AAA group.

CLI (AAA Group Configuration Mode)

radius ip vrf *vrf_name*

no radius ip vrf

Web Element Manager Path

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

radius ip vrf

New command added to configure the parameters for GRE tunnel interface support. This command associates the Virtual Routing and Forwarding (VRF) Context instance for GRE tunnel interface configuration with default AAA group.

CLI (Context Configuration Mode)

ip radius vrf *vrf_name*

no radius ip vrf

Web Element Manager Path

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

radius accounting billing-version

This command configures the billing-system version of RADIUS accounting servers.

CLI (AAA Group & Context Configuration Modes)

radius accounting billing-version *version*

default radius accounting billing-version

Web Element Manager Path

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

radius attribute

New optional keyword added to configure the RADIUS client to sent VLAN ID with nexthop forwarding address to system when running in single nexthop gateway mode.

IMPORTANT

This option is available only when nexthop-forwarding gateway is also configured with **nexthop-forwarding-address** *nexthop_address* keyword and **aaa-large configuration** is enabled at Global Configuration level.

CLI (AAA Server Group Configuration Mode)

[no] radius attribute nas-ip-address address *primary_address* **[nexthop-forwarding-address nexthop_address [vlan** *vlan_id* **]]**

Web Element Manager Path

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

ASN GW Commands - New in Release 9.0

This section provides information on new ASN GW commands available in Release 9.0.

None for this release.

Content Filtering Commands - New in Release 9.0

This section provides information on new commands available in Release 9.0.

None for this release.

ECS Commands - New in Release 9.0

This section provides information on new ECS commands available in Release 9.0.

edr voip-call-end

This command enables generating Event Data Record (EDR) on the completion of voice calls.

CLI (Rulebase Configuration Mode)

edr voip-call-end edr-format *edr_format_name*

{ default | no } edr voip-call-end

Web Element Manager Path

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

group-of-prefixed-urls

This command enables creating/configuring/deleting a group-of-prefixed-URLs.

CLI (Active Charging Service Configuration Mode)

group-of-prefixed-urls *group_name* **[-noconfirm]**

no group-of-prefixed-urls *group_name*

Web Element Manager Path

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

group-of-ruledefs-application

This command specifies the purpose of setting up a group-of-ruledefs as either for charging or for post processing.

CLI (Group-of-Ruledefs Configuration Mode)

group-of-ruledefs-application { charging | post-processing }

no group-of-ruledefs-application

Web Element Manager Path

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

icmp req-threshold

This command configures the maximum number of outstanding ICMP requests to store for ICMP reply matching. This command will be available to all products using Enhanced Charging Service.

CLI (Ruledef Configuration Mode)

icmp req-threshold *threshold*

default icmp req-threshold

Web Element Manager Path

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

icmpv6 any-match

This command defines a rule definition to analyze and charge user traffic based on any match (catch-all) expression for Internet Control Message Protocol Version 6 (ICMPv6).

CLI (Ruledef Configuration Mode)

[no] icmpv6 any-match *operator condition*

Web Element Manager Path

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

icmpv6 code

This command defines a rule definition to analyze and charge user traffic based on the ICMPv6 code.

CLI (Ruledef Configuration Mode)

[no] icmpv6 code *operator code*

Web Element Manager Path

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

icmpv6 type

This command defines a rule definition to analyze and charge user traffic based on the ICMPv6 type.

CLI (Ruledef Configuration Mode)

[no] icmpv6 type *operator type*

Web Element Manager Path

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

ip version

This command specifies a rule definition to analyze and charge user traffic based on the IP version—ipv4 or ipv6.

CLI (Ruledef Configuration Mode)

[no] ip version *operator ip_version*

Web Element Manager Path

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

system-limit

This command configures the system-wide Layer 4 flow limit.

CLI (ACS Configuration Mode)

system-limit l4-flows *limit*

{ default | no } system-limit l4-flows

Web Element Manager Path

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

policy-control burst-size

This command configures the burst size for bandwidth limiting per dynamic-rule or per bearer.

CLI (ACS Configuration Mode)

policy-control burst-size { auto-readjust [duration *duration* **] | bytes** *bytes* **}**

{ default | no } policy-control burst-size

Web Element Manager Path

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

post-processing dynamic

This command configures specified ruledefs/group-of-ruledefs as dynamic post-processing ruledefs/group-of-ruledefs enabling to differentiate between normal post-processing rules from pre-configured ones.

CLI (Rulebase Configuration Mode)

post-processing dynamic { group-of-ruledefs *group_name* **| ruledef** *ruledef_name* **} charging-action** *charging_action* **[description** *description* **]**

no post-processing dynamic { group-of-ruledefs *group_name* **| ruledef** *ruledef_name* **}**

Web Element Manager Path

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

prefixed-url

This command adds URLs to be filtered to a group-of-prefixed-URLs. This command used for the URL Filtering feature, and is available in the new ACS Group-of-Prefixed-URLs Configuration Mode.

CLI (Group-of-Prefixed-URLs Configuration Mode)

[no] prefixed-url *url*

Web Element Manager Path

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

url-preprocessing

This command enables/disables a group-of-prefixed-urls for preprocessing.

CLI (Rulebase Configuration Mode)

[no] url-preprocessing bypass group-of-prefixed-urls *group_name*

Web Element Manager Path

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

Firewall Commands - New in Release 9.0

This section provides information on new commands available in Release 9.0.

firewall icmp-checksum-error

This command configures Stateful Firewall action on packets with ICMP Checksum errors.

CLI (Firewall-and-NAT Policy Configuration Mode)

```
firewall icmp-checksum-error { drop | permit }
default firewall icmp-checksum-error
```

Web Element Manager Path

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

firewall icmp-fsm

This command enables/disables Stateful Firewall's ICMP Finite State Machine (FSM).

CLI (Firewall-and-NAT Policy Configuration Mode)

```
[ default | no ] firewall icmp-fsm
```

Web Element Manager Path

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

firewall ip-reassembly-failure

This command configures Stateful Firewall action on packets involved in IP Reassembly Failure scenarios.

CLI (Firewall-and-NAT Policy Configuration Mode)

```
firewall ip-reassembly-failure { drop | permit }
default firewall ip-reassembly-failure
```

Web Element Manager Path

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

firewall malformed-packets

This command configures Stateful Firewall action on malformed packets.

CLI (Firewall-and-NAT Policy Configuration Mode)

```
firewall malformed-packets { drop | permit }
default firewall malformed-packets
```

Web Element Manager Path

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

firewall tcp-checksum-error

This command configures Stateful Firewall action on packets with TCP Checksum errors.

CLI (Firewall-and-NAT Policy Configuration Mode)

```
firewall tcp-checksum-error { drop | permit }
default firewall tcp-checksum-error
```

Web Element Manager Path

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

firewall tcp-fsm

This command enables/disables Stateful Firewall's TCP Finite State Machine (FSM).

CLI (Firewall-and-NAT Policy Configuration Mode)

```
firewall tcp-fsm [ first-packet-non-syn { drop | permit | send-reset } ]
{ default | no } firewall tcp-fsm
```

Web Element Manager Path

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

firewall tcp-options-error

This command configures Stateful Firewall action on packets with TCP Option errors.

CLI (Firewall-and-NAT Policy Configuration Mode)

```
firewall tcp-options-error { drop | permit }
default firewall tcp-options-error
```

Web Element Manager Path

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

firewall tcp-syn-with-ecn-cwr

This command configures Stateful Firewall action on TCP SYN packets with either ECN or CWR flag set.

CLI (Firewall-and-NAT Policy Configuration Mode)

```
firewall tcp-syn-with-ecn-cwr { drop | permit }
default firewall tcp-syn-with-ecn-cwr
```

Web Element Manager Path

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

firewall udp-checksum-error

This command configures Stateful Firewall action on packets with UDP Checksum errors.

CLI (Firewall-and-NAT Policy Configuration Mode)

```
firewall udp-checksum-error { drop | permit }
```

```
default firewall udp-checksum-error
```

Web Element Manager Path

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

firewall validate-ip-options

This command enables / disables the Stateful Firewall validation of IP options for errors. When enabled, Stateful Firewall will drop packets with IP option errors.

CLI (Firewall-and-NAT Policy Configuration Mode)

```
[ default | no ] firewall validate-ip-options
```

Web Element Manager Path

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

GGSN Commands - New in Release 9.0

This section provides information on new commands available in Release 9.0.

gtpc nsapi-in-create-pdp-response

New command added to configure the inclusion/exclusion of optional IE NSAPI in “Create PDP Context Response” message in GTP-C.

CLI (GGSN Service Configuration Mode)

```
[default | no] gtpc nsapi-in-create-pdp-response
```

Web Element Manager Path

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

gtpc ran-procedure-ready-delay

New command added to configure the GGSN to enable the RAN Procedure Ready feature for the particular GGSN service and specify the timeout period for RAN procedure timer in GGSN which is started on arrival of every secondary Create PDP Context request.

Once a “Create PDP Context Request” is received by GGSN from SGSN, a timer will be started at GGSN and GGSN will wait till the Radio Access Bearer setup is completed and “Update PDP Context Request” is sent by SGSN. If any downlink data is received before arrival of “Update PDP Context Request” or before timer expire, that downlink packets will be queued or buffered.

To support this feature each sub-session uses a common flag ‘ran procedure ready state’, whenever a “Create PDP Context Request” is received for secondary PDP context and sub-session is allocated, this flag will be set to TRUE by default. This common flag is checked while sending downlink traffic, if this flag is FALSE then GGSN permit flow of downlink data but, if it is TRUE, GGSN will queue the downlink packets.

In case if the buffer becomes full (total buffer limit is of 1024 packets) then, all the newly coming packets will be dropped.

If “Update PDP Context Request” is received by GGSN with RAN Procedure flag set or if timer expires the ‘ran-procedure ready state’ flag in sub-session will be reset and hence GGSN will start sending queued packets in ‘first-in first-out’ manner and buffering will be disabled for further downlink traffic.

IMPORTANT

This feature make no effect on Enhanced Charging Service or DPI as the buffering of downlink data is done before sending it to ACSMgr.

IMPORTANT

During SGSN handoff scenario all packets will be processed in a normal way and the downlink packets buffered till the timer expires.

CLI (GGSN Service Configuration Mode)

gtpc ran-procedure-ready-delay [timeout *dur***]**

[default | no] gtpc ran-procedure-ready-delay

Web Element Manager Path

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

gtpc private-extension

New keyword added to configure the overcharging protection when radio coverage lost for a subscriber in a GGSN service.

CLI (GGSN Service Configuration Mode)

gtpc private-extension {{{focs | odb} access-list *acl_name* **in disconnect-on-violation }| ggsn-preservation-mode | insk | loss-of-radio-coverage | none}**

no gtpc private-extension [focs | insk | preservation-mode | loss-of-radio-coverage]

Web Element Manager Path

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

HA Commands - New in Release 9.0

This section provides information on new commands available in Release 9.0.

None for this release.

NAT Commands - New in Release 9.0

This section provides information on new NAT commands available in Release 9.0.

firewall tcp-idle-timeout-action

This command configures action to take on TCP idle timeout expiry. In this release, this CLI configuration is also available to NAT with the "[600-00-7805] *NAT/PAT With DPI*" license.

CLI (Firewall-and-NAT Policy Configuration Mode)

`firewall tcp-idle-timeout-action { drop | reset }`

`{ default | no } firewall tcp-idle-timeout-action`

Web Element Manager Path

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

nat private-ip-flow-timeout

This command configures the Private IP NPU Flow Timeout setting. By default, for NAT-enabled calls the downlink private IP NPU flow will not be installed at call setup for a subscriber session. The flow will only be installed on demand. When there is no traffic on the private flow, the private IP flow will be removed after the configurable timeout period.

CLI (Firewall-and-NAT Policy Configuration Mode)

`nat private-ip-flow-timeout` *`timeout`*

`{ default | no } nat private-ip-flow-timeout`

Web Element Manager Path

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

secondary ip pool

This command specifies a secondary IP pool to be used as backup pool for NAT.

IMPORTANT

This command is license dependent, requiring the [600-00-7871] *NAT Bypass* license. For more information, please contact your local sales representative.

CLI (APN Configuration Mode)

`secondary ip pool` *`pool_name`*

`no secondary ip pool`

Web Element Manager Path

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

PDIF Commands - New in Release 9.0

This section provides information on new commands available in Release 9.0.

None for this release.

PDSN Commands - New in Release 9.0

This section provides information on new commands available in Release 9.0.

l2tp send accounting-correlation-info

New command added to enable the L2TP LAC to send accounting correlation information (Correlation-Id, NAS-IP-Address and NAS-ID) in L2TP control message (ICRQ) during session setup to LNS. LNS can be configured to include this information in ECS billing records, so that billing servers can easily correlate accounting records from PDSN/LAC and LNS.

CLI (Subscriber Configuration Mode)

```
[no | default] l2tp send accounting-correlation-info
```

Web Element Manager Path

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

Peer-to-Peer - New in Release 9.0

This section provides information on new Peer-to-Peer commands in Release 9.0.

p2p-dynamic-rules

This command enables/disables the P2P Dynamic Signature Updates feature.

CLI (ACS Configuration Mode)

p2p-dynamic-rules { { file *location* **[force] } | { protocol [all | bittorrent | directconnect | edonkey | gnutella | skype | yahoo +] } }**

default p2p-dynamic-rules file

no p2p-dynamic-rules { file | protocol [all | bittorrent | directconnect | edonkey | gnutella | skype | yahoo +] }

Web Element Manager Path

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

Session Control Manager Commands - New in Release 9.0

This section provides information on new commands available in Release 9.0.

ipv4-ipv6-interworking

This command allows the IPv4-IPv6 interworking functionality. Default is disabled.

CLI (CSCF Service Configuration Mode)

[no] ipv4-ipv6-interworking

Web Element Manager Path

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

sip-request

This command configures SIP Request-related configuration in a S-CSCF service.

CLI (CSCF Serving-CSCF Configuration Mode)

sip-request re-route { response-code *code* **| max-attempts** *attempts* **}**
default sip-request re-route max-attempts
no sip-request re-route response-code *code*

Web Element Manager Path

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

SGSN Commands - New in Release 9.0

This section provides information on new commands available in Release 9.0.

apn-selection-default

New operator policy command has been added to enable and configure a default APN for use when the normal APN selection process fails.

CLI (SGSN Operator Policy Configuration Mode)

```
apn-selection-default network-identifier <apn_net_id> [
require-subscription-apn network-identifier <apn_net_id>]

noapn-selection-default
```

Web Element Manager Path

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

gtp

New command to enable/disable the GTPC private extension in cases of loss of radio coverage (LORC). This is one of the two commands required to enable the overcharging protection feature.

CLI (SGSN APN Policy Configuration Mode)

```
gtp private-extension loss-of-radio-coverage send-to-ggsn
[send-to-peer-sgsn]

remove gtp private-extension loss-of-radio-coverage
```

Web Element Manager Path

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

gtpp trigger rat-change

SGSN support for this command has been added. This command configures whether or not the RAT change interim CDR is generated for the inter-service handoff

CLI (GTPP Server Group Configuration Mode)

```
[ no ] gtpp trigger rat-change
default gtpp trigger
```

Web Element Manager Path

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

override-arp-with-ggsn-arp

New CLI has been added to enable configuration of the SGSN to negotiate or change or "not" to negotiate or change the value of the ARP received from the GGSN. This configuration of the SGSN will allow the ARP sent by GGSN in CPCR / UPCR / UPCQ to be applicable as an overriding value.

CLI (SGSN Operator Policy Configuration Mode)

```
[ remove] override-arp-with-ggsn-arp
```

Web Element Manager Path

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

ranap

This command enables or disables the inclusion of the paging cause IEs and the modification of paging sources in various RANAP messages.

CLI (RNC Service Configuration Mode)

```
ranap { paging-cause-ie { all | background-data <value> |
conversational-data <value> | gmm-signalling <value>| gs-signalling
<value> | interactive-data <value> | sm-signalling <value> |
sms-signalling <value> | streaming-data <value> } | {
signalling-indication-ie { rab-assignment-request [ relocation-request ]
| relocation-request [ rab-assignment-request ] } }
```

Web Element Manager Path

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

loss-of-radio-coverage ranap-cause

New command to include the detection cause for loss of radio coverage in the Iu Release message. This is one of the two commands required to enable the overcharging protection feature.

CLI (IuPS Service Configuration Mode)

```
loss-of-radio-coverage ranap-cause cause#

default loss-of-radio-coverage ranap-causee
```

Web Element Manager Path

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

ranap

This command enables or disables the inclusion of the Signalling Indication IEs in various RANAP messages depending upon circumstances.

CLI (RNC Service Configuration Mode)

```
ranap { signalling-indication-ie { rab-assignment-request [
relocation-request ] | relocation-request [ rab-assignment-request ] }
```

Web Element Manager Path

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

reset-resource

This command enables the operator to control message length by configuring the number of IuConIDs sent in each RANAP Reset Resource message.

CLI (DNS Client Configuration Mode)

[default] reset-resource max-iuconid-per-msg <*number*>

Web Element Manager Path

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

gtpp dead-server suppress-cdrs

New command defines the action the SGSN will take on the CDRs generated during a communication failure between the SGSN and the GTPP servers.

CLI (GTPP Group Configuration Mode)

[no | default] gtpp dead-server suppress-cdrs

Web Element Manager Path

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

inbound-asp-identifier validate

This command enables or disables the validation of ASP identifiers inbound to the SGSN via routes defined with the SS7 routing domain.

CLI (SS7 Routing Domain Configuration Mode)

inbound-asp-identifier validate

[default | no] inbound-asp-identifier validate

Web Element Manager Path

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

Modified Configuration Commands

This section contains configuration commands that have been modified in Release 9.0. Modified commands in this version are divided into the following sections:

- *Common Commands - Modified in Release 9.0*
- *Content Filtering Commands - Modified in Release 9.0*
- *ECS Commands - Modified in Release 9.0*
- *Firewall Commands - Modified in Release 9.0*
- *GGSN Commands - Modified in Release 9.0*
- *HA Commands - Modified in Release 9.0*
- *NAT Commands - Modified in Release 9.0*
- *PDIF Commands - Modified in Release 9.0*
- *PDSN Commands - Modified for Release 9.0*
- *Peer-to-Peer - Modified for Release 9.0*
- *Session Control Manager Commands - Modified for Release 9.0*
- *SGSN Commands - Modified for Release 9.0*

Common Commands - Modified in Release 9.0

This section provides information on common commands modified for Release 9.0.

configure hd raid

Configures the disk preference when both hard disks on the ST40 have valid RAID information.

CLI (HD Raid Configuration Mode

```
[ default ] select { newer | none } disk [ -noconfirm ]
```

Web Element Manager Path

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

diameter peer-select

This command specifies the Diameter Credit Control primary and secondary host for credit control. This command now enables specifying IMSI prefix or suffix, or IMSI prefix or suffix ranges for peer selection. In this release, this change is only available to UMTS networks.

CLI (Credit Control Configuration Mode)

diameter peer-select peer *peer_name* **[realm** *realm_name***] [secondary-peer** *sec_peer_name* **[realm** *realm_name* **]] [imsi-based { [prefix | suffix]** *imsi/prefix/suffix_start_value* **} [to** *imsi/prefix/suffix_end_value* **]]**

no diameter peer-select [imsi-based { [prefix | suffix] *imsi/prefix/suffix_start_value* **} [to** *imsi/prefix/suffix_end_value* **]**

Web Element Manager Path

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

ip arp

New optional keyword added to associate a Virtual Routing and Forwarding (VRF) context with specific static ARP entry for GRE tunnel interface support.

CLI (Context Configuration Mode)

ip arp *ip_address mac_address* [vrf *vrf_name*]

no ip arp *ip_address*

Web Element Manager Path

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

ip route

New optional keyword added to associate a Virtual Routing and Forwarding (VRF) context with specific static route configuration for GRE tunnel interface support.

CLI (Context Configuration Mode)

[no] ip route {*ip_address/ip_mask* **|** *ip_address ip_mask***}**
{ *gateway_ip_address* **| next-hop** *next_hop_ip_address* **| point-to-point | tunnel}** *egress_intrfc_name* **[cost** *cost* **]**
[precedence *precedence* **] [vrf** *vrf_name***] +**

Web Element Manager Path

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

ospf graceful-restart

Support for OSPF graceful restart has been added to the existing command.

CLI (Global Configuration Mode)

ospf graceful-restart { grace-period *grace_period* | **helper { never | policy { only-reload | only-upgrade } }**

Web Element Manager Path

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

policy-control charging-rule-base-name

This command configures interpretation of Charging-Rule-Base-Name AVP from PCRF either as active-charging rulebase or active-charging group-of-ruledefs. The optional keyword **ignore-when-removed** was added to this command.

When Charging-Rule-Base-Name AVP is interpreted as active-charging rulebase, if PCRF requests the removal of a Charging-Rule-Base-Name, which is the same as the rulebase used for that PDP context, the PDP context is terminated. This is because after removal of the rulebase, the PDP context will have no rulebase. This is the default behavior.

When the **ignore-when-removed** option is configured, PCRF request for removal of Charging-Rule-Base-Name is ignored and no action is taken.

CLI (Active Charging Service Configuration Mode)

policy-control charging-rule-base-name { active-charging-group-of-ruledefs | active-charging-rulebase [ignore-when-removed] }

default policy-control charging-rule-base-name

Web Element Manager Path

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

require active-charging

This command enables/disables Active Charging Service (ACS) with or without Category-based Content Filtering application. The **static-and-dynamic** keyword was added to this command, which for Dynamic Content Filtering support, specifies that the Dynamic Rater Package (model and feature files) must be distributed to rating modules on startup, recovery, etc.

CLI (Global Configuration Mode)

require active-charging [isolated-mode] [content-filtering category [static-and-dynamic]] [optimized-mode]

no require active-charging

Web Element Manager Path

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

radius accounting

This command configures the current context's RADIUS accounting function options. The **stop-only** keyword was added to this command, which specifies archiving of STOP accounting messages only.

CLI (AAA Group & Context Configuration Modes)

radius accounting { archive [stop-only] | deadtime *dead_minutes* **| detect-dead-server { consecutive-failures** *count* **| keepalive | response-timeout** *seconds* **} | interim interval** *seconds* **| max-outstanding** *msgs* **| max-pdu-size** *octets* **| max-retries** *tries* **| max-transmissions** *trans* **| timeout** *idle_seconds* **| unestablished-sessions }**

no radius accounting { archive | detect-dead-server | interim interval | max-transmissions | unestablished-sessions }

default radius accounting { deadtime | detect-dead-server | interim interval seconds | max-outstanding | max-pdu-size | max-retries | max-transmissions | timeout }

Web Element Manager Path

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

snmp target

A new security level, `priv-auth`, has been added to the `snmp target` command to support SNMPv3 notifications. When the security level is set to `priv-auth`, both authentication and encryption are enabled.

CLI (Global Configuration Mode)

```
snmp target name ip_address [ port number ] [ non-default ] [ security-name
string ] [ version { 1 | 2c | 3| view ] [security-level { noauth | { auth |
priv-auth privacy [encrypted] des  } authentication [encrypted] { md5 | sha
}  } } [ informs | traps ]
```

Web Element Manager Path

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

tunnel-mode

New configuration keyword added to create new configuration mode named GRE Tunnel Interface Configuration Mode for GRE interface configuration. Refer *GRE Tunnel Interface Configuration Mode Commands* chapter in *Command Line Interface Reference*.

CLI (Context Configuration Mode)

```
tunnel-mode {gre | ipv6ip}
defualt tunnel-mode
```

Web Element Manager Path

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

Content Filtering Commands - Modified in Release 9.0

This section provides information on Content Filtering commands modified in Release 9.0.

content-filtering mode

This command enables the specified Content Filtering mode within a rulebase. In this release, specifying the static-and-dynamic mode enables dynamic rating in the rulebase after static rating fails.

CLI (Rulebase Configuration Mode)

`content-filtering mode { category { static-only | static-and-dynamic } | server-group` *`cf_server_group`* **`}`**

`no content-filtering mode`

Web Element Manager Path

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

upgrade content-filtering category rater-pkg

This command upgrades the Static Rating Database (SRDB) for Category-based Content Filtering application. The **`rater-pkg`** option was added to this command. This enables manual upgrades of the Dynamic Content-Filtering Rater Package (*rater.pkg* file). The *rater.pkg file* contains the models and feature counters that are used to return the dynamic content rating. The upgrade will trigger distribution of the *rater.pkg* to all the SRDBs.

CLI (Exec Mode)

`upgrade content-filtering category { database | rater-pkg }`

Web Element Manager Path

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

ECS Commands - Modified in Release 9.0

This section provides information on ECS commands modified in Release 9.0.

billing-records

This command configures the type of billing to be performed for subscriber sessions. The rf keyword was added to this command. This keywords enables Rf accounting. Rf accounting is applicable only for dynamic and predefined rules that are marked for it. Dynamic rules have a field offline-enabled to indicate this. To mark a predefined rule as offline-enabled, use this keyword and the billing-action CLI in the Charging Action Configuration Mode.

CLI (Rulebase Configuration Mode)

`billing-records { egcdr | radius | rf | udr udr-format` *`udr_format_name`* **`} +`**

`no billing-records`

Web Element Manager Path

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

ftp command id

This command defines a rule definition to analyze and charge user traffic based on FTP command ID. This release onwards, the command identifier for a rule definition can be specified as an integer from 0 through 18.

CLI (Ruledef Configuration Mode)

`[ no ] ftp command id` *`operator command_id`*

Web Element Manager Path

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

ftp command name

This command defines a rule definition to analyze and charge user traffic based on FTP command name. This release onwards, the following options are supported for FTP analyzer:

- **`eprt`**: eprt command
- **`epsv`**: epsv command

CLI (Ruledef Configuration Mode)

`[ no ] ftp command name` *`operator command_name`*

Web Element Manager Path

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

ip dst-address

This command defines a rule definition to analyze and charge user traffic based on IP destination address. This command now accepts IPv6 addresses.

CLI (Ruledef Configuration Mode)

[no] ip dst-address { *operator* **{** *ip_address* **|** *ip_address/mask* **} | { !range | range } host-pool** *host_pool* **}**

Web Element Manager Path

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

ip protocol

This command configures the IP protocol setting for a packet filter. The **range** keyword option to select a range of protocols is now obsoleted.

CLI (Packet Filter Configuration Mode)

ip protocol = *protocol_number*

no ip protocol

Web Element Manager Path

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

ip protocol

This command defines a rule definition to analyze and charge user traffic based on the protocol being transported by IP packets. This command now accepts **icmpv6** protocol option.

CLI (Ruledef Configuration Mode)

[no] ip protocol *operator* **{** *protocol_assignment* **| ah | esp | gre | icmp | icmpv6 | tcp | udp }**

Web Element Manager Path

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

ip remote-address

This command configures IP remote address setting for a packet filter. The **range** keyword option to select a range of IP addresses is now obsoleted.

CLI (Packet Filter Configuration Mode)

ip remote-address = { *ip_address* **|** *ip_address/mask* **}**

no ip remote-address

Web Element Manager Path

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

ip server-ip-address

This command defines a rule definition to analyze and charge user traffic matching the IP address of the destination, i.e. from the subscriber, of the connection. This command now accepts IPv6 addresses.

CLI (Ruledef Configuration Mode)

[no] ip server-ip-address { *operator* **{** *ip_address* **|** *ip_address/mask* **} | { !range | range } host-pool** *host_pool* **}**

Web Element Manager Path

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

ip src-address

This command defines a rule definition to analyze and charge user traffic based on IP source address. This command now accepts IPv6 addresses.

CLI (Ruledef Configuration Mode)

[no] ip src-address { *operator* **{** *ip_address* **|** *ip_address/mask* **} | { !range | range } host-pool** *host_pool* **}**

Web Element Manager Path

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

ip subscriber-ip-address

This command defines a rule definition to analyze and charge user traffic matching the IP address of the subscriber (either source address or destination address). This command now accepts IPv6 addresses.

CLI (Ruledef Configuration Mode)

[no] ip subscriber-ip-address { *operator* **{** *ip_address* **|** *ip_address/mask* **} | { !range | range } host-pool** *host_pool* **}**

Web Element Manager Path

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

post-processing priority

This command configures the post-processing action to be taken on the specified ruledef in the rulebase. The **group-of-ruledefs** keyword was added to the command. This enables assigning the specified group-of-ruledefs to the rulebase.

CLI (Rulebase Configuration Mode)

post-processing priority *priority* **{ group-of-ruledefs** *group_name* **| ruledef** *ruledef_name* **} charging-action** *charging_action_name* **[description** *description* **]**

no post-processing priority *priority*

Web Element Manager Path

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

rule-variable

This command specifies the event rule variable for EDR file format attribute. The following new rule variable options were added to this command:

- **ip**:
  - **version**
- **icmpv6**:
  - **code**
  - **type**
- **traffic-type**
- **voip-duration**

CLI (EDR Format Configuration Mode)

rule-variable *protocol rule* **priority** *priority* **[in-quotes]**

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

Web Element Manager Path

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

Firewall Commands - Modified in Release 9.0

This section provides information on commands modified for Release 9.0.

None for this release.

GGSN Commands - Modified in Release 9.0

This section provides information on GGSN commands modified in Release 9.0.

gtpp storage-server local file

New keyword **custom8** added to define customized CDR file format It uses *node-id-suffix_date_time_fixed-length-seq-num*.u format for file naming where:

- *date* is date in MMDDYYYYY (01312010) for mat
- *time* is time in HHMMSS (023508) format
- *fixed-length-seq-num* is the fixed length of sequence number for specific file having 6 digit counter starting from 000001 and end to 999999. Once file sequence reached to 999999 the sequence will be reset to 000001.

CLI (GTPP Server Group Configuration Mode)

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

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

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

Web Element Manager Path

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

authentication

New optional keywords **username-strip-apn** and **password-use-pco** added to configure support for AAA Auth user name as MSISDN/IMSI and password as PCO received password for APN.

CLI (APN Configuration Mode)

authentication {[msid-auth | imsi-auth [username-strip-apn] [password-use-pco] | msisdn-auth [username-strip-apn] [password-use-pco]]| [allow-noauth][chap preference][mschap preference] [pap preference]}

default authentication

Web Element Manager Path

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

HA Commands - Modified in Release 9.0

This section provides information on HA commands modified in Release 9.0.

None for this release.

NAT Commands - Modified in Release 9.0

This section provides information on NAT commands modified in Release 9.0.

access-rule

With the NAT-only license [600-00-7805] *NAT/PAT With DPI*, the **trigger open-port** keyword is no longer available with this command. In the earlier releases, for NAT this keyword was not functional.

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* **] } | priority** *priority* **{ [dynamic-only | static-and-dynamic] access-ruledef** *ruledef_name* **{ deny [charging-action** *charging_action* **] | permit [bypass-nat | nat-realm** *nat_realm* **] } } }**

default access-rule no-ruledef-matches { downlink | uplink } action

no access-rule priority *priority*

Web Element Manager Path

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

ip pool

IMPORTANT

This change is applicable to UMTS deployments in StarOS 9.0, and for CDMA deployments in StarOS 8.3.

This command enables adding, modifying, and deleting an IP address pool in the current context. The following keywords and associated options were added to this command for the Network Address Translation (NAT) feature:

- **nat-one-to-one**: This keyword and associated options enable configuring one-to-one NAT realms.
- **napt-users-per-ip-address**: This keyword and associated options enable configuring many-to-one NAT realms.

The following keyword and associated options were removed from this command:

- **nat-realm**

IMPORTANT

On upgrading from StarOS 8.1 to StarOS 9.0, all NAT realms configured in StarOS 8.1 using the **nat-realm** keyword must in StarOS 9.0 be reconfigured using one of the following keywords:

- nat-one-to-one
- napt-users-per-ip-address

For example, the following command in StarOS 8.1 configuration:
ip pool *pool1* **range** *11.22.33.44 55.66.77.88* **nat-realm ...**

must in StarOS 9.0 be reconfigured to one of the following:
ip pool *pool1* **range** *11.22.33.44 55.66.77.88* **nat-one-to-one ...**
ip pool *pool1* **range** *11.22.33.44 55.66.77.88* **napt-users-per-ip-address ...**

CLI (Context Configuration Mode)

ip pool *name* **{** *ip_address subnet_mask* **|** *ip_addr_mask_combo* **| range** *start_ip_address end_ip_address* **} [private [** *priority* **] | public [** *priority* **] | static] [tag { none | pdif-setup-addr }] [address-hold-timer** *seconds* **| alert-threshold [group-available | pool-free | pool-hold | pool-release | pool-used]** *low_thresh* **[clear** *high_thresh* **]] [group-name** *group_name* **] [include-nw-bcast] [nat** *priority* **] [nexthop-forwarding-address** *ip_address* **[overlap vlanid** *vlan_id* **] [nw-reachability server** *server_name* **] [respond-icmp-echo** *ip_address* **] [resource] [send-icmp-dest-unreachable] [explicit-route-advertise] [srp-activate] [suppress-switchover-arp] [unicast-gratuitous-arp-address** *ip_address* **] [policy allow-static-allocation] [nat-one-to-one [[alert-threshold [{ pool-free | pool-hold | pool-release | pool-used }** *low_thresh* **[clear** *high_thresh* **] +] [nat-binding-timer** *binding_timer* **] [on-demand] [send-nat-binding-update] +] | napt-users-per-ip-address** *users* **[[alert-threshold [{ pool-free | pool-hold | pool-release | pool-used }** *low_thresh* **[clear** *high_thresh* **] +] [max-chunks-per-user** *chunks* **] [nat-binding-timer** *timer* **] [on-demand] [port-chunk-size** *size* **] [port-chunk-threshold** *chunk_threshold* **] [send-nat-binding-update] +]**

no ip pool *name* **[tag { none | pdif-setup-addr }] [address-hold-timer | alert-threshold [group-available | pool-free | pool-hold | pool-release | pool-used]] [group-name] [include-nw-bcast] [nexthop-forwarding-address] [nw-reachability server] [respond-icmp-echo** *ip_address* **] [send-icmp-dest-unreachable] [explicit-route-advertise] [send-nat-binding-update] [srp-activate] [suppress-switchover-arps] [unicast-gratuitous-arp-address] [policy allow-static-allocation]**

Web Element Manager Path

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

PDIF Commands - Modified in Release 9.0

This section provides information on PDIF commands modified in Release 9.0.

control-dont-fragment

This command controls the don’t fragment (DF) bit in the outer IP header of the IPsec tunnel data packet.

CLI (Crypto Map Manuel Configuration Mode)

```
default set control-dont-fragment { clear-bit | copy-bit | set-bit }
```

Web Element Manager Path

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

PDSN Commands - Modified for Release 9.0

This section provides information on PDSN commands modified in Release 9.0.

None for this release.

Peer-to-Peer - Modified for Release 9.0

This section provides information on Peer-to-Peer commands modified in Release 9.0.

p2p-detection protocol

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

- gtalk
- oovoo

CLI (ACS Configuration Mode)

```
[ no ] p2p-detection protocol [ all | applejuice | ares | bittorrent |
ddlink | directconnect | edonkey | fasttrack | feidian | filetopia | fring
| gadugadu | gnutella | gtalk | halflife2 | hamachivpn | imesh | irc |
iskoot | jabber | manolito | msn | mute | oovoo | orb | oscar | pando | popo
| pplive | ppstream | qq | qqlive | skinny | skype | slingbox | sopcast |
soulseek | steam | tvants | tvuplayer | uusee | vpnx | vtun | winmx | winny
| wofwarcraft | xbox | yahoo | zattoo ] +
```

Web Element Manager Path

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

p2p-detection protocol

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

- freenet
- aimini
- battlefld
- openft
- qqgame
- quake
- secondlife
- actsync
- nimbuzz
- iax
- paltalk
- warcft3
- rdp
- iptv
- pandora

CLI (ACS Configuration Mode)

[no] p2p-detection protocol [all | applejuice | ares | bittorrent | ddlink | directconnect | edonkey | fasttrack | feidian | filetopia | fring | gadugadu | gnutella | gtalk | halflife2 | hamachivpn | imesh | irc | iskoot | jabber | manolito | msn | mute | oovoo | orb | oscar | pando | popo | pplive | ppstream | qq | qqlive | skinny | skype | slingbox | sopcast | soulseek | steam | tvants | tvuplayer | uusee | vpnx | vtun | winmx | winny | wofwarcraft | xbox | yahoo | zattoo | freenet | aimini | battlefld | openft | qqgame | quake | secondlife | actsync | nimbuzz | iax | paltalk | warcft3 | rdp | iptv | pandora] +

Web Element Manager Path

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

show active-charging analyzer statistics

This command displays the statistics for protocol analyzers. The following new protocols were added to this command:

- freenet
- aimini
- battlefld
- openft
- qqgame
- quake
- secondlife
- actsync
- nimbuzz
- iax
- paltalk
- warcft3
- rdp
- iptv
- pandora

CLI (Exec Mode)

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

Web Element Manager Path

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

show active-charging flows

This command displays information for active charging flows. The following new protocols were added to this command for the **type** keyword:

- freenet
- aimini
- battlefld
- openft
- qqgame
- quake
- secondlife
- actsync
- nimbuzz
- iax
- paltalk
- warcft3
- rdp
- iptv
- pandora

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 statistics for specific active charging service sessions. The following new protocols were added to this command for the **type** keyword:

- freenet
- aimini
- battlefld
- openft
- qqgame

- quake
- secondlife
- actsync
- nimbuzz
- iax
- paltalk
- warcft3
- rdp
- iptv
- pandora

CLI (Exec Mode)

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

Web Element Manager Path

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

p2p protocol

This command configures the system to detect specific P2P protocols for charging purposes. The following new protocols were added to this command:

- freenet
- aimini
- battlefld
- openft
- qqgame
- quake
- secondlife
- actsync
- nimbuzz
- iax
- paltalk
- warcft3
- rdp
- iptv
- pandora

CLI (Exec Mode)

[no] p2p protocol *operator protocol*

Web Element Manager Path

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

Session Control Manager Commands - Modified for Release 9.0

The following commands have been modified in Release 9.0.

bind

The **use-serviceport-towards-network** keyword has been added.

CLI (CSCF Service Configuration Mode)

bind address *ip_address* **[access-ipsec-crypto-template** *template* **]**
[cscf-hostname *host_name* **] [max-sessions** *max#* **] [port** *number* **]**
[reserved-call-capacity *percentage*] **[transport tcp] [**
use-serviceport-towards-network]

no bind address

Web Element Manager Path

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

diameter

The **request-timeout** *sec*, **Rq-custom, and Rx-rel8** keywords have been added.

CLI (CSCF Proxy-CSCF Configuration Mode)

diameter location-info { dictionary { e2custom01 | e2custom02 | e2custom03
| e2custom04 | e2custom05 | e2custom06 | e2custom07 | e2custom08 |
e2custom09 | e2standard } | origin endpoint *endpoint_name* **| peer-select**
peer *peer_name* **[peer-realm** *realm_name* **] [secondary-peer** *peer_name*
[sec-peer-realm *realm_name* **]] | request-timeout** *sec* **}**

diameter policy-control { dictionary { Gq-custom | Gq-standard | Rq-custom|
Rx-rel8 | Rx-standard | Tx-standard | custom01 | custom02 | custom03 |
custom04 | custom05 | custom06 | custom07 | custom08 | custom09 } |
origin endpoint *endpoint_name* **| peer-select peer** *peer_name* **[peer-realm**
realm_name **] [secondary-peer** *peer_name* **[sec-peer-realm** *realm_name* **]] |**
request-timeout *sec* **}**

default diameter { location-info | policy-control } { dictionary |
request-timeout }

no diameter { location-info | policy-control } [origin endpoint |
peer-select]

Web Element Manager Path

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

SGSN Commands - Modified for Release 9.0

The following commands have been modified in Release 9.0.

gmm

The Inter-SGSN RAU TRAU timer is now configurable for both 2G and 3G SGSNs with a range of 5 to 60 seconds.

CLI (GPRS Service Configuration Mode)

gmm trau-timeout seconds

default gmm trau-timeout

CLI (SGSN Service Configuration Mode)

gmm trau-timeout seconds

default gmm trau-timeout

Web Element Manager Path

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

llc

The **n201u-max** keyword has been added to the **llc** command to allow the operator to set the maximum size that can be negotiated for the downlink data packet (information field length for U/UI frames.

CLI (GPRS Service Configuration Mode)

llc { iov-ui-in-xid-reset | n201u-max | pdu-lifetime *secs* **| T200 sapi1** *time* **| T200 sapi11 t** *time* **| T200 sapi3** *time* **| T200 sapi5** *time* **| T200 sapi7** *time* **| T200 sapi9** *time* **}**

Web Element Manager Path

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

llc

The **uplink-pdu-len-validation** keyword has been added to the **llc** command to provide the operator the ability to validate or ignore the negotiated uplink N201_U packet size.

CLI (GPRS Service Configuration Mode)

llc { iov-ui-in-xid-reset | n201u-max | pdu-lifetime *secs* **| T200 sapi1** *time* **| T200 sapi11 t** *time* **| T200 sapi3** *time* **| T200 sapi5** *time* **| T200 sapi7** *time* **| T200 sapi9** *time* | **uplink-pdu-len-validation }**

no llc uplink-pdu-len-validation

Web Element Manager Path

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

rnc id

The SGSN now supports the Extended RNC Id IE from Release 7. The maximum range was 4095 and has now been increased to 65535.

CLI (IuPS Service Configuration Mode)

rnc id <*0 - 65535***>**

Web Element Manager Path

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

qos prefer-as-cap

The **qos** command, in the SGSN operator policy's APN policy configuration mode, has been modified to support capping of the local QoS bit rate when the subscribed QoS provided by the HLR is lower than the locally configured value.

CLI (IuPS Service Configuration Mode)

qos { class | prefer-as-cap { hlr-subscription | local | both-hlr-and-local } | rate-limit }

remove qos prefer-as-cap

Web Element Manager Path

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

apn/apn-selection-default/wildcard-apn

To meet 3GPP TS23.003, the maximum length for the network-identifier for all APN definitions has been reduced from 63 characters to 62.

CLI (SGSN Operator Policy Configuration Mode)

apn { network-identifier *apn_net_id* **| operator-identifier** *apn_op_id* **}**

Web Element Manager Path

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

application-context-name

The range for the Gf 1-in-N IMEI check event timer has been expanded to 1 -30 seconds from 15 - 30 seconds; keeping 15 seconds as the default.

CLI (SGSN Operator Policy Configuration Mode)

application-context-name *application* **operator timer** *time*

Web Element Manager Path

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

Obsoleted Commands

This section contains configuration commands that have been obsoleted in Release 9.0. Obsoleted commands in this version are divided into the following sections:

- *Common Commands - Obsoleted in Release 9.0*
- *Content Filtering Commands - Obsoleted in Release 9.0*
- *ECS Commands - Obsoleted in Release 9.0*
- *Firewall Commands - Obsoleted in Release 9.0*
- *GGSN Commands - Obsoleted in Release 9.0*
- *HA Commands - Obsoleted in Release 9.0*
- *PDSN Commands - Obsoleted in Release 9.0*
- *SGSN Commands - Obsoleted in Release 9.0*

Common Commands - Obsoleted in Release 9.0

This section provides information on commands that are common to all products that were obsoleted in Release 9.0.

css acsmgr-selection-attempts

With the external CSS server feature no longer being supported, this command has been obsoleted.

CLI (Global Configuration Mode)

`[ default ] css acsmgr-selection-attempts` *`num_attempts`*

Web Element Manager Path

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

css delivery-sequence

With the external CSS server feature no longer being supported, this command has been obsoleted.

CLI (Global Configuration Mode)

`css delivery-sequence` *`name`* **`[ -noconfirm ]`**

`no css delivery-sequence` *`name`*

Web Element Manager Path

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

css service

With the external CSS server feature no longer being supported, this command has been obsoleted.

CLI (Global Configuration Mode)

css service *name* **[-noconfirm]**

no css service *name*

Web Element Manager Path

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

css server

With the external CSS server feature no longer being supported, this command has been obsoleted.

CLI (Context Configuration Mode)

css server *name* **keepalive [interval** *seconds* **] [local-address** *localIP* **] [num-retry** *number* **] [protocol { icmp | tcp }] [remote-address** *remIP* **] [timeout** *seconds* **]**

no css server *name*

Web Element Manager Path

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

redirect css delivery-sequence

With the external CSS server feature no longer being supported, this command has been obsoleted.

CLI (ACL Configuration Mode)

redirect css delivery-sequence *sequence_name* **{** *options* **}**

Web Element Manager Path

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

redirect css delivery-sequence

With the external CSS server feature no longer being supported, this command has been obsoleted.

CLI (IPv6 ACL Configuration Mode)

redirect css delivery-sequence *sequence_name* **{** *options* **}**

Web Element Manager Path

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

Content Filtering Commands - Obsoleted in Release 9.0

This section provides information on CF commands that were obsoleted in Release 9.0.

None for this release.

ECS Commands - Obsoleted in Release 9.0

This section provides information on ECS commands that were obsoleted in Release 9.0.

None for this release.

Firewall Commands - Obsoleted in Release 9.0

This section provides information on Firewall commands that were obsoleted in Release 9.0.

firewall tcp-first-packet-non-syn

This command configures the action to take on TCP flows starting with a non-syn packet. In StarOS 9.0, this command is deprecated. This configuration is now available as the "**`firewall tcp-fsm [ first-packet-non-syn { drop | permit | send-reset } ]`**" command.

CLI (Firewall-and-NAT Configuration Mode)

`firewall tcp-first-packet-non-syn { drop | reset }`

`default firewall tcp-first-packet-non-syn`

Web Element Manager Path

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

GGSN Commands - Obsoleted in Release 9.0

This section provides information on GGSN commands that were obsoleted in Release 9.0.

None for this release.

HA Commands - Obsoleted in Release 9.0

This section provides information on HA commands that were obsoleted in Release 9.0.

None for this release.

PDSN Commands - Obsoleted in Release 9.0

This section provides information on PDSN commands that were obsoleted in Release 9.0.

None for this release.

SGSN Commands - Obsoleted in Release 9.0

This section provides information on SGSN commands that were obsoleted in Release 9.0.

authenticate attach

The **attach** keyword has been modified and the **inter-rat** keyword has been included to enable or disable (default) authentication for Inter-RAT Attaches.

CLI (SGSN Operator Policy Configuration Mode)

authenticate { attach [inter-rat [access-type *gprs* **|** *umts* **]] }**

default authenticate attach inter-rat [access-type *gprs* **|** *umts* **]**

Web Element Manager Path

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

authenticate rau update-type

The **authentica rau update-type** command has been enhanced to include the **with inter-rat-local-ptmsi** qualifier to enable or disable (default) authentication for Inter-RAT RAUs.

CLI (SGSN Operator Policy Configuration Mode)

authenticate rau update-type { ra-update with inter-rat-local-ptmsi | combined-update with inter-rat-local-ptmsi | imsi-combined-update with inter-rat-local-ptmsi }

default authenticate rau update-type { ra-update | combined-update | imsi-combined-update }

Web Element Manager Path

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

GTPP Storage Server (GSS)

This section provides information on GSS changes in Release 9.0.

GSS Changes in Release 9.0

This section provides information on GSS changes in Release 9.0.

None for this release.

Web Element Manager Changes

This section provides information on Web Element Manager changes in Release 9.0.

None for this release.

CHAPTER 4
ACCOUNTING MANAGEMENT

This section contains additions and changes made to the accounting-related parameters available in Release 9.0. Topics covered in this chapter are:

- *Bulk Statistic Enhancements in Release 9.0*
- *CDR Enhancements*
- *Command Enhancements*
- *New Commands*
- *RADIUS Attributes in Release 9.0*
- *Diameter Attributes in Release 9.0*
- *Web Element Manager Enhancements*

Bulk Statistic Enhancements in Release 9.0

This section lists bulk statistic additions and changes in Release 9.0. 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 9.0.

APN Schema

- inexcd-mbr-pkt-drop
- outexcd-mbr-pkt-drop
- inexcd-gbr-pkt-drop
- outexcd-gbr-pkt-drop
- inexcd-ambr-pkt-drop
- outexcd-ambr-pkt-drop
- inmisc-pkt-drop
- outmisc-pkt-drop
- inexcd-mbr-byte-drop
- outexcd-mbr-byte-drop
- inexcd-gbr-byte-drop
- outexcd-gbr-byte-drop
- inexcd-ambr-byte-drop
- outexcd-ambr-byte-drop
- inmisc-byte-drop
- outmisc-byte-drop

CSCF Schema

- total-roaming-ue-regs
- total-roaming-ue-succ-regs
- total-roaming-ue-fail-regs
- total-roaming-ue-regs-403
- total-roaming-ue-re-regs
- total-roaming-ue-succ-re-regs
- total-roaming-ue-fail-re-regs
- total-roaming-ue-re-regs-403

- total-roaming-ue-de-regs
- total-roaming-ue-succ-de-regs
- total-roaming-ue-fail-de-regs
- total-roaming-ue-de-regs-403
- call-resp-3xxrx
- call-resp-3xxtx
- call-resp-402rx
- call-resp-402tx
- call-resp-403rx
- call-resp-403tx
- call-resp-404rx
- call-resp-404tx
- call-resp-407rx
- call-resp-407tx
- call-resp-408rx
- call-resp-408tx
- call-resp-420rx
- call-resp-420tx
- call-resp-421rx
- call-resp-421tx
- call-resp-480rx
- call-resp-480tx
- call-resp-486rx
- call-resp-486tx
- call-resp-487rx
- call-resp-487tx
- call-resp-488rx
- call-resp-488tx
- call-resp-4xxrx
- call-resp-4xxtx
- call-resp-500rx
- call-resp-500tx
- call-resp-503rx
- call-resp-503tx
- call-resp-5xxrx
- call-resp-5xxtx
- call-resp-6xxrx
- call-resp-6xxtx

- migrated-tcp-conn
- packet-tcp-rx
- packet-tcp-tx
- bytes-tcp-rx
- bytes-tcp-tx
- message-tcp-request-rx
- message-tcp-request-tx
- message-tcp-response-rx
- message-tcp-response-tx
- message-tcp-mtu-switch
- perf-att-init-reg
- perf-att-init-reg-3gpp-geran
- perf-att-init-reg-3gpp-utran-fdd
- perf-att-init-reg-3gpp2-1x
- perf-att-init-reg-ieee-80211a
- perf-att-init-reg-ieee-80211b
- perf-att-init-reg-other-at
- perf-succ-init-reg
- perf-succ-init-reg-3gpp-geran
- perf-succ-init-reg-3gpp-utran-fdd
- perf-succ-init-reg-3gpp2-1x
- perf-succ-init-reg-ieee-80211a
- perf-succ-init-reg-ieee-80211b
- perf-succ-init-reg-other
- perf-fail-init-reg
- perf-fail-init-reg-401
- perf-fail-init-reg-403
- perf-fail-init-reg-404
- perf-fail-init-reg-420
- perf-fail-init-reg-500
- perf-fail-init-reg-other
- perf-mean-init-reg-setup
- perf-att-rereg
- perf-att-rereg-3gpp-geran
- perf-att-rereg-3gpp-utran-fdd
- perf-att-rereg-3gpp2-1x
- perf-att-rereg-ieee-80211a
- perf-att-rereg-ieee-80211b

- perf-att-rereg-other-at
- perf-succ-rereg
- perf-succ-rereg-3gpp-geran
- perf-succ-rereg-3gpp-utran-fdd
- perf-succ-rereg-3gpp2-1x
- perf-succ-rereg-ieee-80211a
- perf-succ-rereg-ieee-80211b
- perf-succ-rereg-other
- perf-fail-rereg
- perf-fail-rereg-401
- perf-fail-rereg-403
- perf-fail-rereg-404
- perf-fail-rereg-420
- perf-fail-rereg-500
- perf-fail-rereg-other
- perf-att-dereg-ue
- perf-att-dereg-ue-3gpp-geran
- perf-att-dereg-ue-3gpp-utran-fdd
- perf-att-dereg-ue-3gpp2-1x
- perf-att-dereg-ue-ieee-80211a
- perf-att-dereg-ue-ieee-80211b
- perf-att-dereg-ue-other-at
- perf-succ-dereg-ue
- perf-succ-dereg-ue-3gpp-geran
- perf-succ-dereg-ue-3gpp-utran-fdd
- perf-succ-dereg-ue-3gpp2-1x
- perf-succ-dereg-ue-ieee-80211a
- perf-succ-dereg-ue-ieee-80211b
- perf-succ-dereg-ue-other
- perf-fail-dereg-ue
- perf-fail-dereg-ue-401
- perf-fail-dereg-ue-403
- perf-fail-dereg-ue-404
- perf-fail-dereg-ue-420
- perf-fail-dereg-ue-500
- perf-fail-dereg-ue-other
- perf-att-dereg-hss
- perf-succ-dereg-hss

- perf-fail-dereg-hss
- perf-fail-dereg-hss-401
- perf-fail-dereg-hss-403
- perf-fail-dereg-hss-404
- perf-fail-dereg-hss-420
- perf-fail-dereg-hss-500
- perf-fail-dereg-hss-other
- perf-att-dereg-serv
- perf-succ-dereg-serv
- perf-fail-dereg-serv
- perf-fail-dereg-serv-401
- perf-fail-dereg-serv-403
- perf-fail-dereg-serv-404
- perf-fail-dereg-serv-420
- perf-fail-dereg-serv-500
- perf-fail-dereg-serv-other
- perf-att-3rdparty-reg
- perf-succ-3rdparty-reg
- perf-fail-3rdparty-reg
- perf-fail-3rdparty-reg-401
- perf-fail-3rdparty-reg-403
- perf-fail-3rdparty-reg-404
- perf-fail-3rdparty-reg-420
- perf-fail-3rdparty-reg-500
- perf-fail-3rdparty-reg-other
- perf-att-uar
- perf-succ-uaa
- perf-fail-uaa
- perf-att-sar
- perf-succ-saa
- perf-fail-saa
- perf-att-session
- perf-succ-session-180
- perf-succ-session-200
- perf-ans-session
- perf-fail-session
- perf-att-lir
- perf-succ-lia

- perf-fail-lia
- perf-att-session-frm-oth-domain
- perf-frbdn-session-frm-oth-domain
- perf-att-session-to-oth-domain
- perf-frbdn-session-to-oth-domain
- perf-att-init-reg-visited
- perf-frbdn-init-reg-visited
- perf-rmg-users-out
- perf-att-mar
- perf-succ-maa
- perf-fail-maa
- perf-att-ppr
- perf-succ-ppa
- perf-fail-ppa
- perf-att-subscribe
- perf-succ-subscribe
- perf-fail-subscribe
- perf-att-notify
- perf-succ-notify
- perf-fail-notify
- de2a-session-init
- de2a-session-active
- de2a-udr-sent
- de2a-uda-received
- de2a-uda-err-3xxx
- de2a-uda-parse-err
- de2a-udr-err

DCCA Schema

The DCCA schema was added.

- vpnname
- vpnid
- ipaddr
- port
- ccr-inisent
- cca-inirec
- cca-initimeout
- ccr-updsent
- cca-updrec

- cca-updtimeout
- ccr-tersent
- cca-terrec
- cca-tertimeout
- reauth-anssent
- reauth-reqrec

DPCA Schema

The DPCA schema was added.

- vpnname
- vpnid
- ipaddr
- port
- ccr-inisent
- cca-inirec
- ccr-initimeout
- ccr-updsent
- cca-updrec
- ccr-updtimeout
- ccr-tersent
- cca-terrec
- ccr-tertimeout
- reauth-anssent
- reauth-reqrec

eGTP-C Schema

- tun-sent-retransbearrescmd-fail
- tun-recv-retransbearrescmd-fail

GPRS Schema

- llc-frame-stats-ui-gea1-ciph-data-frames-rx
- llc-frame-stats-ui-gea1-ciph-data-frames-tx
- llc-frame-stats-ui-gea1-ciph-data-octets-rx
- llc-frame-stats-ui-gea1-ciph-data-octets-tx
- llc-frame-stats-ui-gea2-ciph-data-frames-rx
- llc-frame-stats-ui-gea2-ciph-data-frames-tx
- llc-frame-stats-ui-gea2-ciph-data-octets-rx
- llc-frame-stats-ui-gea2-ciph-data-octets-tx
- llc-frame-stats-ui-gea3-ciph-data-frames-rx
- llc-frame-stats-ui-gea3-ciph-data-frames-tx

- llc-frame-stats-ui-gea3-ciph-data-octets-rx
- llc-frame-stats-ui-gea3-ciph-data-octets-tx
- llc-frame-stats-ui-unciph-rx
- llc-frame-stats-ui-unciph-tx
- llc-frame-stats-ui-unciph-data-frames-rx
- llc-frame-stats-ui-unciph-data-frames-tx
- llc-frame-stats-ui-unciph-data-octets-rx
- llc-frame-stats-ui-unciph-data-octets-tx
- gprs-num-subs-gea0-capable
- gprs-num-subs-gea1-capable
- gprs-num-subs-gea2-capable
- gprs-num-subs-gea3-capable
- gprs-num-subs-gea0-negotiated
- gprs-num-subs-gea1-negotiated
- gprs-num-subs-gea2-negotiated
- gprs-num-subs-gea3-negotiated

MIPv6HA Schema

- admprohreason-authoptmiss
- admprohreason-hbitnotset
- admprohreason-invaaaspi
- admprohreason-invhaspi
- admprohreason-polrej
- admprohreason-notauth
- admprohreason-noperm
- insufresource-nosessmgr
- insufresource-nomem
- insufresource-sessmgrrej
- insufresource-ipqexc
- insufresource-simbindexc

P-GW Schema

The P-GW schema was added.

S-GW Schema

The S-GW schema was added.

System Schema

- discover-dis-parse-err
- request-dis-parse-err

- release-dis-parse-err
- fng-cursess
- fng-curactive
- fng-curdormant
- fng-ttlsetup
- fng-curchildsa
- disc-reason-395
- disc-reason-396
- disc-reason-397
- disc-reason-398
- disc-reason-399
- disc-reason-400
- disc-reason-401
- disc-reason-402
- disc-reason-403
- disc-reason-404
- disc-reason-405
- disc-reason-406
- disc-reason-407
- disc-reason-408
- disc-reason-409
- disc-reason-410
- disc-reason-411

SGSN Schema

- 3G-service-rej-unknown-cause
- 2G-primary-actv-fail
- 2G-secondary-actv-fail
- 3G-total-attach-fail-all
- 2G-total-attach-fail-all
- 3G-intra-comb-rau-fail-iu_release
- 3G-intra-comb-rau-fail-ongoing-proc
- 2G-intra-comb-rau-fail-ongoing-proc
- 3G-inter-comb-rau-fail-iu_release
- 3G-inter-comb-rau-fail-ongoing-proc
- 2G-inter-comb-rau-fail-ongoing-proc
- mt-sms-in-queue
- relay-prot-err-protocol-error-rx
- relay-prot-smma-rx

Modified Bulk Statistics

The following bulk statistics were modified in Release 9.0.

None for this release.

Obsoleted Bulk Statistics

The following bulk statistics were obsoleted in Release 9.0.

SGSN Schema

- 2G-service-rej-sem-wrong-msg

SGTP Schema:

- ggsn-address

Web Element Manager Path

Click Accounting | Bulk Statistics Configuration.

CDR Enhancements

This section lists new custom GTPP dictionaries in Release 9.0. Refer to the *AAA Interface Configuration and Reference* for details.

IPv6 Support in S-CDRs in custom11

IPV6 support is added for the custom11 dictionary in SGSN. With the introduction of this the custom11 now can support either IPV6 or IPV4 served PDP addresses. To support this, PDPType and ServedPDPAddress fields have been changed.

- **pdpType:** IPV6 or IPV4
- **servedPDPAddress:** up to 16 bytes

SGSN Support for custom17

custom17 defined CDR fields are now supported in SGSN S-CDRs. A complete listing of the fields is included in the *SGSN and Mobility Management Charging Detail Record Field Reference Tables* chapter of the *AAA Interface and Administration Reference.*

Command Enhancements

None for this release.

New Commands

None for this release.

RADIUS Attributes in Release 9.0

This section lists additions and changes to RADIUS AVPs in Release 9.0. Refer to the *AAA Interface Configuration and Reference* for details.

New Attributes

The following RADIUS attributes are new in Release 9.0.

- DHCPMSG-Server-IP
- DHCP-RK
- DHCP-RK-Key-ID
- DHCP-RK-Lifetime
- hLMA-IPv6-PMIP6
- Hotline-Profile-ID
- Hotline-Session-Timer
- HTTP-Redirection-Rule
- IP-Redirection-Rule
- NAS-Filter-Rule
- PMIP6-RK-KEY
- PMIP6-RK-SPI
- PMIP6-Service-Info
- SN-CF-Call-RoamingInternatnl
- SN-Fast-Reauth-Username
- SN-QOS-HLR-Profile
- WiMAX-Home-HNP-PMIP6
- WiMAX-Home-IPv4-HoA-PMIP6

Modified Attributes

The following RADIUS attributes were modified in Release 9.0.

- 3GPP-PDP-Type
- Acct-Termination-Cause
- NAS-Port-Type
- SN1-Disconnect-Reason
- SN1-PPP-Progress-Code
- SN1-Service-Type
- SN-Disconnect-Reason
- SN-PPP-Progress-Code
- SN-Service-Type
- WiMAX-PPAQ

Removed Attributes

The following RADIUS attributes were removed in Release 9.0.

None for this release.

Diameter Attributes in Release 9.0

This section lists additions and changes to Diameter attributes in Release 9.0. Refer to the *AAA Interface Reference* for details.

New Attributes

The following Diameter attributes are new in Release 9.0.

- 3GPP-CF-IPv6-Address
- 3GPP-SGSN-IPv6-Address
- 3GPP2-Allowed-Persistent-TFTS
- 3GPP2-BSID
- 3GPP2-Correlation-Id
- 3GPP2-Information
- 3GPP2-Inter-User-Priority
- 3GPP2-MEID
- 3GPP2-Max-Auth-Aggr-BW-BET
- 3GPP2-Max-Inst-Per-Service-Option
- 3GPP2-Max-Per-Flow-Priority-User
- 3GPP2-Max-Svc-Inst-Link-Flow-Total
- 3GPP2-RAT-Type
- 3GPP2-RP-Session-ID
- 3GPP2-Service-Option
- 3GPP2-Service-Option-Profile
- 3GPP2-Serving-PCF
- 3GPP2-User-Zone
- Access-Network-Type
- Access Network Type
- Access-Restriction-Data
- Alert-Reason
- Alert Reason.
- All-APN-Configurations-Included-Indicator
- Allocation-Retention-Priority
- AMBR
- AN-GW-Address
- AN-Trusted
- ANID
- APN-Aggregate-Max-Bitrate-DL
- APN-Aggregate-Max-Bitrate-UL
- APN-Authorized

- APN-Barring-Type
- APN-Configuration
- APN-Configuration-Profile
- APN-OI-Replacement
- ARP
- Authentication-Info
- Auth-Profile-Id-Bi-Direction
- Auth-Profile-Id-Forward
- Auth-Profile-Id-Reverse
- AUTN
- Call-Barring-Info-List
- Cancellation-Type
- Change-Condition
- Change-Time
- Chargeable-User-Id
- Charging-Rule-Name-LI
- Civic-Location
- Client-Identity
- CoA-Information
- CoA-IP-Address
- Complete-Data-List-Included-Indicator
- Context-Identifier
- CSG-Id
- CSG-Subscription-Data
- Diagnostics
- DSA-Flags
- DSR-Flags
- Dynamic-Address-Flag
- EUTRAN-Vector
- Event-Report-Indication
- Expiration-Date
- Extended-QoS-Filter-Rule
- External-Client
- Feature-List-ID-Resp
- Feature-List-Resp
- FID
- Flow-Information
- Flow-Label

- Geospatial-Location
- GERAN-Vector
- GMLC-Address
- GMLC-Restriction
- GPRS-Subscription-Data
- HPLMN-ODB
- IDA-Flags
- IDR-Flags
- IMEI
- Item-Number
- KASME
- KC-Key
- LCS-Info
- LCS-PrivacyException
- Line-Identifier
- Local-Sequence-Number
- Location-Information
- Logical-Access-Id
- MEID
- MIP-Home-Agent-Address-IETF
- MIP-Home-Agent-Host
- MIP6-Agent-Info
- MIP6-Feature-Vector
- MIP6-Home-Link-Prefix
- MO-LR
- Mobile-Node-Identifier
- Node-Id
- NOR-Flags
- Notification-To-UE-User
- OMC-Id
- Operator-Determined-Barring
- Operator-String
- Packet-Filter-Content
- Packet-Filter-Identifier
- Packet-Filter-Information
- Packet-Filter-Operation
- PDP-Context
- PDP-Type

- Physical-Access-Id
- PLMN-Client
- PMIP-Mobile-Node-Address
- Pre-emption-Capability
- Pre-emption-Vulnerability
- Priority-Level
- QoS-Capability
- QoS-Negotiation
- QoS-Profile-Template
- QoS-Resource-Identifier
- QoS-Resource-Operation
- QoS-Resource-Request
- QoS-Resources
- QoS-Rule-Definition
- QoS-Rule-Install
- QoS-Rule-Name
- QoS-Rule-Remove
- QoS-Rule-Report
- QoS-Subscribed
- QoS-Upgrade
- RACS-Contact-Point
- RAND
- RAS-Id
- RAT-Frequency-Selection-Priority
- RAT-Frequency-Selection-Priority.
- Re-Synchronization-Info
- Regional-Subscription-Zone-Code
- Requested-EUTRAN-Authentication-Info
- Requested-GERAN-Authentication-Info
- Requested-Information
- Resource-Allocation-Notification
- Roaming-Restricted-Due-To-Unsupported-Feature
- Sector-Id
- Security-Parameter-Index
- Service-Data-Container
- Service-Selection
- Service-Specific-Info
- ServiceTypeIdentity

- SGW-Change
- Software-Version
- Specific-APN-Info
- SRES
- SS-Code
- SS-Status
- STN-SR
- Subscriber-Priority
- Subscriber-Status
- Subscription-Data
- Supported-Features-Resp
- Supported-RAT-Type
- Teleservice-List
- Terminal-Information
- Terminal-Type
- Time-First-Usage
- Time-Last-Usage
- Time-Usage
- Traffic-Data-Volumes
- TS-Code
- Tunnel-Header-Filter
- Tunnel-Header-Length
- Tunnel-Information
- ULA-Flags
- ULR-Flags
- UMTS-Vector
- User-Id
- UTRAN-Vector
- Vendor-Id-Resp
- Vendor-Specific-QoS-Profile-Template
- Visited-PLMN-Id
- VPLMN-Dynamic-Address-Allowed
- XRES

Modified Attributes

The following Diameter attributes were modified in Release 9.0.

- 3GPP-PDP-Type
- Charging-Rule-Install

- Event-Trigger
- Experimental-Result-Code
- Final-Unit-Indication
- QoS-Rule-Install
- Specific-Action
- Trace-Data

Removed Attributes

The following Diameter attributes were removed in Release 9.0.

None for this release.

Web Element Manager Enhancements

None for this release.

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*
- *Modified Commands*
- *Obsoleted Commands*
- *GTPP Storage Server Changes*
- *Web Element Manager Changes*

New Commands

This section contains performance management commands that are new in Release 9.0. New commands in this version are divided into the following sections:

- *Common Commands - New in Release 9.0*
- *Content Filtering Commands - New in Release 9.0*
- *ECS Commands - New in Release 9.0*
- *Firewall Commands - New in Release 9.0*
- *GGSN Commands - New in Release 9.0*
- *HA Commands - New in Release 9.0*
- *NAT Commands - New in Release 9.0*
- *PDIF Commands - New in Release 9.0*
- *PDSN Commands - New in Release 9.0*
- *Peer-to-Peer - New in Release 9.0*
- *SGSN Commands - New in Release 9.0*

Common Commands - New in Release 9.0

The following common commands are new in Release 9.0.

None for this release.

Content Filtering Commands - New in Release 9.0

The following Content Filtering commands are new in Release 9.0.

None for this release.

ECS Commands - New in Release 9.0

The following ECS commands are new in Release 9.0.

None for this release.

Firewall Commands - New in Release 9.0

The following Stateful Firewall commands are new in Release 9.0.

None for this release.

GGSN Commands - New in Release 9.0

The following GGSN commands are new in Release 9.0.

show apn counter ip-allocation

New command added to display IP allocation method information/statistics counters on per apn basis for all currently active calls.

CLI (Exec Mode)

show apn counter ip-allocation [all | name *apn_name*] [|{**grep** *grep_options* **| more}]**

Web Element Manager Path

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

show ip interface

New keyword **gre-keepalive** added to this command to display states and statistics of GRE keepalive requests for GRE tunnel interface type IP interfaces.

CLI (Exec Mode)

show ip interface [vrf *vrf-name*] **[name** *intfc_name* **[statistics] [tunnel [gre-keepalive]] [summary] [| { grep** *grep_options* **| more }]**

Web Element Manager Path

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

HA Commands - New in Release 9.0

The following HA commands are new in Release 9.0.

None for this release.

NAT Commands - New in Release 9.0

The following NAT commands are new in Release 9.0.

None for this release.

PDIF Commands - New in Release 9.0

The following PDIF commands are new in Release 9.0.

None for this release.

PDSN Commands - New in Release 9.0

The following PDSN commands are new in Release 9.0.

None for this release.

Peer-to-Peer - New in Release 9.0

The following P2P commands are new in Release 9.0.

show active-charging p2p-dynamic-rules

This command displays P2P Dynamic signature file information.

CLI (Exec Mode)

show active-charging p2p-dynamic-rules [verbose] [acsmgr instance *instance_id* **] [| { grep** *grep_options* **| more }]**

Web Element Manager Path

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

SGSN Commands - New in Release 9.0

The following SGSN commands are new in Release 9.0.

None for this release.

Modified Commands

This section contains performance management commands that have been modified in Release 9.0. Modified commands in this version are divided into the following sections:

- *Common Commands - Modified in Release 9.0*
- *Content Filtering Commands - Modified in Release 9.0*
- *ECS Commands - Modified in Release 9.0*
- *Firewall Commands - Modified in Release 9.0*
- *GGSN Commands - Modified in Release 9.0*
- *HA Commands - Modified in Release 9.0*
- *NAT Commands - Modified in Release 9.0*
- *PDIF Commands - Modified in Release 9.0*
- *PDSN Commands - Modified in Release 9.0*
- *Peer-to-Peer Commands - Modified in Release 9.0*
- *Session Control Manager Commands - Modified in Release 9.0*
- *SGSN Commands - Modified in Release 9.0*

Common Commands - Modified in Release 9.0

The following common commands have been modified in Release 9.0.

clear active-charging credit-control statistics

This command clears Credit Control statistics. The **server** keyword and options were added to this command. This enables clearing per Diameter server statistics of Gy messages.

CLI (Exec Configuration Mode)

clear active-charging credit-control statistics [group *group_name* **] [server { ip-address** *ip_address* **[port** *port_number* **] | name** *server_name* **}]**

Web Element Manager Path

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

clear crypto

New **ipsec-3gpp-cscf** keyword added.

CLI (Exec Configuration Mode)

clear crypto { isakmp [tag *map_name* **| peer** *peer_ip* **] | security-association { counters tag** *map_name* **[tx | rx] | tag** *map_name* **| peer** *peer_ip* **} | statistics { ikev2 | ipsec-3gpp-cscf } [service-ip-address** *ip-address* **| service-name** *name* **] }**

Web Element Manager Path

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

clear ims-authorization policy-control

This command clears statistics for all or for a specified IMS Authorization Service or server. The **server** keyword and options were added to this command, which enables to select a specific server.

CLI (Exec Configuration Mode)

clear ims-authorization { policy-control statistics [service *ims_auth_svc_name* **| server { ip-address** *ip_address* **[port** *port_value* **] | name** *server_name* **}] | service statistics [name** *service_name* **] } [| { grep** *grep_options* **| more }]**

Web Element Manager Path

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

monitor protocol

Activates monitor function to examine protocol-specific information based on protocol. The following protocol was added to the list of protocols:

- ICAP

CLI (Exec Mode)

monitor protocol

Web Element Manager Path

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

monitor subscriber username

Activates monitor function to examine protocol-specific information based on subscriber within current context. The following protocol was added to the list of protocols:

- ICAP

CLI (Exec Mode)

monitor subscriber username *user_name*

Web Element Manager Path

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

show active-charging credit-control

This command displays Credit Control statistics. The **server** keyword and options were added to this command. This enables to view per Diameter server statistics of Gy messages.

CLI (Exec Configuration Mode)

show active-charging credit-control { { statistics [group *group_name* **] [server { ip-address** *ip_address* **[port** *port_number* **] | name** *server_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 fw-and-nat policy name

This command displays the Firewall-and-NAT Policy information. The output of this command now includes the following new fields with NAT related configurations and Firewall feature level configurations added:

- Action upon receiving TCP SYN packet with ECN/CWR Flag set
- Action upon receiving a malformed packet
- Action upon IP Reassembly Failure
- Action upon receiving an IP packet with invalid Options
- Action upon receiving a TCP packet with invalid Options
- Action upon receiving an ICMP packet with invalid Checksum
- Action upon receiving a TCP packet with invalid Checksum
- Action upon receiving an UDP packet with invalid Checksum
- TCP Stateful Checks
  - First Packet Non-SYN Action
- ICMP Stateful Checks
- NAT Configuration
  - NBR Format
  - Private IP NPU Flow Timeout
  - Suppress sending NAT bind update to AAA

CLI (Exec Mode)

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

Web Element Manager Path

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

show ims-authorization policy-control

This command displays information and statistics specific to policy control in IP Multimedia Subsystem (IMS) authorization service. The **server** keyword and options were added to this command, which enables to select a specific server.

CLI (Exec Mode)

show ims-authorization policy-control statistics [service *ims_auth_svc_name* **| server { ip-address** *ip_address* **[port** *port_value* **] | name** *server_name* **}] [| { grep** *grep_options* **| more }]**

Web Element Manager Path

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

show rohc

Modified command to add summary output and support HSGW-RoHC.

CLI (Exec Mode)

show rohc { counters [all | callid *call_id* **| msid** *msid_num* **|**
imsi *imsi_num* **| username** *user_name* **] | statistics | summary [all | callid** *call_id* **| msid** *msid_num* **| imsi** *imsi_num* **| username** *user_name* **] } [| { grep** *grep_options* **| more }]**

Web Element Manager Path

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

Content Filtering Commands - Modified in Release 9.0

The following Content Filtering commands have been modified in Release 9.0.

clear content-filtering category statistics

This command clears all Category-based Content Filtering application statistics, or statistics for a specific SRDB Manager instance. This release onwards the SRDB Manager instance number can be specified as any integer from 1 through 10000.

CLI (Exec Mode)

clear content-filtering category statistics [facility srdbmgr instance *instance_value* **]**

Web Element Manager Path

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

show active-charging content-filtering category statistics

This command displays category-based content filtering statistics for rulebase(s). The following Dynamic Content Filtering feature related fields were added to the output of this command:

- Cumulative Dynamic Content Filtering Statistics
  - Dynamic Flows discarded
  - Dynamic Flows redirected
  - Dynamic Flows allowed
  - Dynamic Flows terminated
  - Dynamic Flows discarded with content insertion
  - Total Dynamic Flows blocked
  - Total Number of dynamic lookups
  - Total number of unknown URLs
- Dynamic Failure Action (Rating Attempts Not Completed):
  - Flows discarded
  - Flows redirected
  - Flows allowed
  - Flows terminated
  - Flows discarded with content insertion
  - Total Flows blocked
  - Time taken for Dynamic rating
  - Number of URLs
  - Attempts not completed

CLI (Exec Mode)

show active-charging content-filtering category statistics [rulebase { name *rulebase_name* **| all }] [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 content-filtering server-group statistics

This command displays information for Content Filtering Server Group(s) configured in the service. The following changes were made to this command:

- The **verbose** option was added. This enables viewing ICAP queue length statistics.
- The output of this command now displays the histogram of ICAP server's response time.

CLI (Exec Mode)

show active-charging content-filtering server-group [statistics [verbose]] [name *cfsg_name* **] [| { grep** *grep_options* **| more }]**

Web Element Manager Path

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

show content-filtering category database facility srdbmgr

This command displays details of the specified category-based content filtering database for content filtering application configured in a system/service. The following Dynamic Content Filtering feature related fields were added to the output of this command:

- Dynamic SRDB Instance
- RaterPkg Load Status
- Number of Model files
- Standby Dynamic SRDB Instance
- RaterPkg Load Status
- Number of Model files

CLI (Exec Mode)

show content-filtering category database facility srdbmgr { all | instance *instance_value* **} [verbose] [| { grep** *grep_options* **| more }]**

Web Element Manager Path

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

show content-filtering category statistics facility srdbmgr

This command displays statistics for the Category-based Content Filtering application configured in a system/service. The following Dynamic Content Filtering feature related fields were added to the output of this command:

- Dynamic Content Filtering SRDB Instance Based Statistics:
  - Instance Number
  - Dynamic Rating:
  - Request Count
  - Response Total
  - Response Successful

- Response Not Rated

CLI (Exec Mode)

show content-filtering category statistics facility srdbmgr { all | instance *instance_value* **} [| { grep** *grep_options* **| more }]**

Web Element Manager Path

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

show content-filtering category url <url> policy-id <id> verbose

This command displays the category-based content filtering statistics at the specific URL configured in a system/service. The output of this command now includes the following new fields with Dynamic CF enabled/disabled:

- Action Configured
- Content Insertion String
- Redirect URL

CLI (Exec Mode)

show content-filtering category url *url_string*
[policy-id *cf_policy_id* **| rulebase** *rulebase_name* **] [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 content-filtering category statistics

This command displays the category-based content filtering statistics. The output of this command now includes the following new field for dynamic rating only if the response code is in the range 2xx:

- Response codes not in range 2xx

CLI (Exec Mode)

show active-charging content-filtering category statistics [rulebase { name *rulebase_name* | all **}] [verbose] [| { grep** *grep_options* **| more }]**

Web Element Manager Path

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

show content-filtering category statistics facility srdbmgr all

This command displays the statistics for category-based content filtering application configured in a system/service. The output of this command now includes the following new Dynamic Content Filtering feature related field:

- Histogram for number of URLs hit per SN category (sorted on no. of URLs)

CLI (Exec Mode)

show content-filtering category statistics [facility srdbmgr { all | instance *instance_value* **}]** [| { grep grep_options | **more }]**

Web Element Manager Path

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

show active-charging content-filtering category statistics

This command displays the category-based content filtering statistics. The output of this command now includes the following new fields:

- Number of Packets Hit per Category
- Number of Packets Blocked per Category

CLI (Exec Mode)

show active-charging content-filtering category statistics [rulebase { name *rulebase_name* | all **}] [verbose] [| { grep** *grep_options* **| more }]**

Web Element Manager Path

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

ECS Commands - Modified in Release 9.0

The following ECS commands have been modified in Release 9.0.

show active-charging service

This command displays Active Charging Service details. The output of this command includes the following new field:

- Dynamic Content Filtering: Indicates whether Dynamic Content Filtering is enabled or disabled.

CLI (Exec Mode)

show active-charging service { all | name *svc_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 analyzer statistics

This command displays statistic information for protocol analyzers. The following fields were added to this command's output:

- IPv6
- ICMPv6
- ACS IPv6 Session Stats:
  - Total Uplink Bytes
  - Total Downlink Bytes
  - Total Uplink Pkts
  - Total Downlink Pkts
  - Uplink Bytes Fragmented
  - Downlink Bytes Fragmented
  - Uplink Pkts Fragmented
  - Downlink Pkts Fragmented
  - Uplink Bytes Invalid
  - Downlink Bytes Invalid
  - Uplink Pkts Invalid
  - Downlink Pkts Invalid
- ACS ICMPv6 Session Stats:
  - Total Uplink Bytes
  - Total Downlink Bytes
  - Total Uplink Pkts
  - Total Downlink Pkts
  - ECHO Request
  - ECHO Reply

- Dst Unreachable
- Parameter Problem
- Time Exceeded
- Packet Too Big
- Other ICMP Req
- Invalid Pkts

CLI (Exec Mode)

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

Web Element Manager Path

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

show active-charging analyzer statistics name

This command displays Active Charging protocol analyzer statistics for the specified analyzer. The **ipv6** and **icmpv6** keywords were added to this command.

CLI (Exec Mode)

show active-charging analyzer statistics name { dns | file-transfer | ftp | http | icmp | icmpv6 | imap | ip | ipv6 | mms | p2p | pop3 | rtcp | rtp | rtsp | sdp | secure-http | sip | smtp | tcp | udp | wsp | wtp } [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 analyzer statistics name dns

This command displays Active Charging protocol analyzer statistics for the DNS analyzer. With the support for IPv6 in ACS, AAAA record type is supported in DNS for IPv6 addresses. The output of this command now includes the following new fields corresponding to support AAAA record type in DNS for IPv6:

- Request:
  - AAAA Query Type
- Response:
  - AAAA Query Type

CLI (Exec Mode)

show active-charging analyzer statistics name dns [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 full all

This command displays statistics for Active Charging Service Sessions. The output of this command includes the following new fields:

- Client-IP
- Current IPv6 Flows
- Current ICMPv6 Flows

CLI (Exec Mode)

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

Web Element Manager Path

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

show active-charging flows type

This command displays information on flows filtered by flow type of application protocol. The ipv6 and icmpv6 options were added to this command.

CLI (Exec Mode)

show active-charging flows type { dns | ftp | http | icmp | icmpv6 | imap | ip | ipv6 | mms | p2p | pop3 | rtcp | rtp | rtsp | secure-http | sip | smtp | tcp | udp | unknown | wsp-connection-less | wsp-connection-oriented } [*options* **] [| { 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 ip-address

This command displays active charging flows in a system or service. This command now accepts IPv6 addresses.

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 rulebase statistics

This command displays statistical information for all/the specified rulebase. The output of this command now includes the following new field:

- EDRs generated for voip call end

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.

Firewall Commands - Modified in Release 9.0

The following Stateful Firewall commands have been modified in Release 9.0.

show active-charging firewall statistics verbose

This command displays the Active Charging Stateful Firewall statistics. The output of this command now includes the following new field to control the behavior of Firewall on receiving TCP SYN packets with either ECE/CWR Flags set:

- SYN Packets Dropped due to ECE/CWR Set

CLI (Exec Mode)

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

Web Element Manager Path

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

GGSN Commands - Modified in Release 9.0

The following GGSN commands have been modified in Release 9.0.

show subscribers ggsn-only summary

Following counters added to the output of this command to display the statistics for the overcharging protection support due to loss of radio coverage (LORC):

- out packet dropped due to lorc
- ggsn LORC state

CLI (Exec Mode)

`show subscribers ggsn-only [summary]`

Web Element Manager Path

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

show subscribers ggsn-only full

Following counters added to the output of this command to display the statistics for the overcharging protection support due to loss of radio coverage (LORC):

- GGSN LORC State
- output pkts dropped due to lorc

CLI (Exec Mode)

`show subscribers ggsn-only full`

Web Element Manager Path

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

show gtpc full

Following counter added to the output of this command to display the statistics for the overcharging protection support due to loss of radio coverage (LORC):

- Transitions to LORC state

CLI (Exec Mode)

`show gtpc full`

Web Element Manager Path

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

show gtpc statistics

New keyword **`custom2`** and following counters added to the output of this command with filter **`custom2`** to display the statistics for the overcharging protection support due to loss of radio coverage (LORC):

- LORC Stats
- Sessions in lorc state
- Transitions to lorc state

CLI (Exec Mode)

show gtpc statistics [apn-name *apn_name* **] [custom1 | custom2] [sgsn-address** *address* **] [ggsn-service** *svc_name* **] [verbose]**

Web Element Manager Path

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

HA Commands - Modified in Release 9.0

The following HA commands have been modified in Release 9.0.

None for this release.

NAT Commands - Modified in Release 9.0

The following NAT commands have been modified in Release 9.0.

None for this release.

PDIF Commands - Modified in Release 9.0

The following PDIF commands have been modified in Release 9.0.

None for this release.

PDSN Commands - Modified in Release 9.0

The following PDSN commands have been modified in Release 9.0.

None for this release.

Peer-to-Peer Commands - Modified in Release 9.0

The following Peer-to-Peer commands have been modified in Release 9.0.

None for this release.

show active-charging rulebase statistics name

This command displays details of the active-charging rulebase statistics configured in a system/service. The output of this command now includes the following new fields to support Random Drop as a charging action to degrade voice quality:

- P2P random drop stats
  - Total Dropped Packets
  - Total Dropped Packet Bytes

CLI (Exec Mode)

show active-charging rulebase { { { all | name *rulebase_name* **} [service name** *acs_service* **] } | 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 analyzer statistics name p2p verbose

This command displays details of the active-charging statistics for protocol analyzers configured in a system/service. The output of this command now includes the following fields to support the new protocols:

- Freenet
- Aimini
- Battlefld
- Openft
- Qqgame
- Quake
- Secondlife
- Actsync
- Nimbuzz
- Iax
- Paltalk
- Warcft3
- Rdp
- Iptv
- Pandora

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

This command displays the statistics for Active Charging service sessions. The output of this command now includes the following fields to support the new P2P protocols:

- Current FREENET Sessions
- Current AIMINI Sessions
- Current BATTLEFIELD Sessions
- Current OPENFT Sessions
- Current QQGAME Sessions
- Current QUAKE Sessions
- Current SECONDLIFE Sessions
- Current ACTIVESYNC Sessions
- Current NIMBUZZ Sessions
- Current IAX Sessions
- Current PALTALK Sessions
- Current WARCRAFT3 Sessions
- Current IPTV Sessions
- Current RDP Sessions
- Current PANDORA Sessions

CLI (Exec Mode)

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

Web Element Manager Path

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

show active-charging sessions summary type p2p

This command displays the statistics for specific Active Charging service sessions. The output of this command now includes the following fields to support the new P2P protocols:

- Current FREENET Sessions
- Current AIMINI Sessions
- Current BATTLEFIELD Sessions
- Current OPENFT Sessions
- Current QQGAME Sessions

- Current QUAKE Sessions
- Current SECONDLIFE Sessions
- Current ACTIVESYNC Sessions
- Current NIMBUZZ Sessions
- Current IAX Sessions
- Current PALTALK Sessions
- Current WARCRAFT3 Sessions
- Current IPTV Sessions
- Current RDP Sessions
- Current PANDORA Sessions

CLI (Exec Mode)

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

Web Element Manager Path

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

Session Control Manager Commands - Modified in Release 9.0

The following SCM commands have been modified in Release 9.0.

None for this release.

SGSN Commands - Modified in Release 9.0

The following SGSN commands have been modified in Release 9.0.

None for this release.

Obsoleted Commands

This section contains performance management commands that have been obsoleted in Release 9.0. Obsoleted commands in this version are divided into the following sections:

- *Common Commands - Obsoleted from Release 9.0*
- *Content Filtering Commands - Obsoleted from Release 9.0*
- *ECS Commands - Obsoleted from Release 9.0*
- *Firewall Commands - Obsoleted from Release 9.0*
- *GGSN Commands - Obsoleted from Release 9.0*
- *HA Commands - Obsoleted from Release 9.0*
- *NAT Commands - Obsoleted from Release 9.0*
- *PDSN Commands - Obsoleted from Release 9.0*
- *Peer-to-Peer Commands - Obsoleted from Release 9.0*
- *SGSN Commands - Obsoleted from Release 9.0*

Common Commands - Obsoleted from Release 9.0

The following common commands have been obsoleted in Release 9.0.

show css delivery-sequence

With the external CSS server feature no longer being supported, this command has been obsoleted.

CLI (Exec Mode)

show css delivery-sequence{ all | name *seq_name* **}**

Web Element Manager Path

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

show css server

With the external CSS server feature no longer being supported, this command has been obsoleted.

CLI (Exec Mode)

show css server { all | name *server_name* **}**

Web Element Manager Path

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

show css service

With the external CSS server feature no longer being supported, this command has been obsoleted.

CLI (Exec Mode)

show css service { all | name *service_name* **}**

Web Element Manager Path

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

Content Filtering Commands - Obsoleted from Release 9.0

The following Content Filtering commands have been obsoleted in Release 9.0.

None for this release.

ECS Commands - Obsoleted from Release 9.0

The following ECS commands have been obsoleted in Release 9.0.

None for this release.

Firewall Commands - Obsoleted from Release 9.0

The following Stateful Firewall commands have been obsoleted in Release 9.0.

None for this release.

GGSN Commands - Obsoleted from Release 9.0

The following GGSN commands have been obsoleted in Release 9.0.

None for this release.

HA Commands - Obsoleted from Release 9.0

The following HA commands have been obsoleted in Release 9.0.

None for this release.

NAT Commands - Obsoleted from Release 9.0

The following NAT commands have been obsoleted in Release 9.0.

None for this release.

PDSN Commands - Obsoleted from Release 9.0

The following PDSN commands have been obsoleted in Release 9.0.

None for this release.

Peer-to-Peer Commands - Obsoleted from Release 9.0

The following Peer-to-Peer commands have been obsoleted in Release 9.0.

None for this release.

SGSN Commands - Obsoleted from Release 9.0

The following SGSN commands have been obsoleted in Release 9.0.

None for this release.

GTPP Storage Server Changes

The following commands have been modified in Release 9.0.

show gtpp storage-server status

This command displays details of the configured GTPP storage server. The following new fields have been added to the output of this command to support additional disks monitored by GSS, and to monitor the GSS Disk partition space:

- Resource Monitor:
  - Available Disk Gss Datafile Path (GB)
  - Available Disk Gss Install Path (GB)
  - Available Disk Gss Database Path (GB)
- Resource Monitor Status:
  - Available Disk Gss Datafile Path (GB)
  - Available Disk Gss Install Path (GB)
  - Available Disk Gss Database Path (GB)

CLI (Exec Mode)

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

Web Element Manager Path

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

show gtpp storage-server streaming file statistics

New counter `Total Files Failed` added to indicate the number of CDR files failed for streaming due to any reason to remote storage.

CLI (Exec Mode)

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

Web Element Manager Path

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

show gtpp storage-server streaming file statistics verbose

New counter **CDR distribution in DRT Messages** added to indicate the distribution of CDRs in DRT messages.

CLI (Exec Mode)

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

Web Element Manager Path

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

Web Element Manager Changes

There were no Web Element Manager changes in Release 9.0.

CHAPTER 6
SECURITY MANAGEMENT

This section contains additions and changes made to the security features available in Release 9.0.

Security Enhancements

New Commands

The following new commands were added for Release 9.0.

None for this release.

Modified Commands

The following commands were modified in Release 9.0.

None for this release.

Obsoleted Commands

The following commands were obsoleted in Release 9.0.

None for this release.