Release 7.x to Release 8.x Change Reference

Version 7.x-8.x

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-22956-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

Reorient or relocate the receiving antenna.

Increase the separation between the equipment and receiver.

Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

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

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

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

Release 7.x to Release 8.x Change Reference

© 2010 Cisco Systems, Inc. and/or its affiliated entities. All rights reserved.

TABLE OF CONTENTS

About This Guide

Conventions Used xxviii
Contacting Customer Support xxx

Chapter 1: New Feature Summary

Common Features in Release 8.0 1-2
Configurable Transmit Timing Source 1-2
CDR PUSH Transfer Mode 1-2
DHCP Service Support with MPLS Labels 1-3
Four-Port Gigabit Ethernet Line Card (QGLC) 1-3
Hard Disk Support on SMC Card in ST40 Platform 1-4
"monitor protocol" CLI Command Option to use with HDD Configuration 1-4
Link Aggregation 1-4
New SNMP MIB Objects and Traps 1-4
New Bulk Statistics 1-4
New RADIUS Attributes 1-5
Configuration and Performance Parameter Enhancements 1-5
Software Patch Upgrades Not Supported 1-5
Common Features in Release 8.1 1-6
Duplicate CDR Detection 1-6
Intelligent Packet Monitoring System (IPMS) 1-6
Domain-based L2TP Tunnel Support 1-7
Software Patch Upgrades Not Supported 1-7
Common Features in Release 8.3 1-8
Packet Services Card 2 1-8
10 Gigabit Ethernet Line Card 1-9
ASN GW Features in Release 8.0 1-10
ASN GW Features in Release 8.1 1-11
Multi-host Support 1-11
Content Filtering in Release 8.0 1-12
Content Filtering in Release 8.1 1-13
URL Blacklisted Content Filtering 1-13
ECS Features in Release 8.0 1-14
Group of Ruledefs Configuration Mode 1-14
IP Readdressing 1-14
Packet Filter Configuration Mode 1-14
Corrected DCCA Behavior upon Receipt of Charging-Rule-Base-Name AVP 1-14
Pipelining of HTTP Requests 1-15
ECS Features in Release 8.1 1-16
Enhanced Charging Service in Optimized Mode 1-16

EDR Generation in Flow-end and Transaction Complete Scenarios with sn-volume Fields 1-17
Origin-host Encoding for Optimized Mode 1-17
Number of TCP Connections for Optimized Mode 1-18
ASR in Rel. 7 Gx Implementation Not Supported 1-18
Charging Rule Definition Rejection if Precedence AVP Missing in Create Case 1-18
Pipelining of HTTP Requests 1-18
Default IP for Unsupported Protocol 1-18
ESS Features in Release 8.0 1-19
ESS Features in Release 8.1 1-20
Support for Ignoring Insignificant UDRs 1-20
Support for Multiple Content Types 1-20
Support for Pushing of xDR Files 1-20
Support for Forwarding SNMP Traps to Multiple Destinations 1-20
Firewall Features in Release 8.0 1-21
ACS and Stateful Firewall Integration 1-21
Firewall Ruledef Configuration Mode 1-21
Host Pool, IMSI Pool, and Port Map Support in ACS 1-21
Licensing 1-21
Firewall Features in Release 8.1 1-22
Network Address Translation (NAT) 1-22
Policy-based Firewall and NAT Functionality 1-22
Upgrading to Release 8.1 1-23
GGSN Features in Release 8.0 1-24
Multimedia Broadcast Multicast Service (MBMS) 1-24
Network Controlled QoS (NCQoS) 1-25
Traffic Shaping 1-25
Direct Tunnel Support 1-25
Highest Preference to LNS for DNS Value 1-26
CCR (T) Sent after Receiving “Diameter-Credit-Limit-Reached” at Message Level in CCA (I) after Upgrade to v8.0 1-27
GGSN Features in Release 8.1 1-28
Hard Disk Storage for CDR Files 1-28
NPU Assisted MBMS Data Flow 1-28
Rel. 7 Gx Interface Support 1-28
Quad Gig-E Line Card (QGLC) & Link Aggregation 1-29
GGSN Behavior on QOS Change 1-29
Secondary GTPP Group and Enable/Disable CDR Archiving 1-29
Configuring Secondary GTPP Group under the APN 1-29
Enabling/disabling CDR Archiving in GTPP Group 1-29
Transport Layer Protocol Selection over Ga Interface 1-30
Benefits 1-30
Description 1-30
NSAPI Encoding in Diameter 1-30
GSS Features in Release 8.0 1-31
Menu-Driven Installation 1-31

SGSN Support 1-31
custom4 Format 1-31
GSS Features in Release 8.1 1-32
Support for New File Formats 1-32
Archive Mode Functionality 1-32
Support for GTPP Custom Dictionary 1-32
HA Features in Release 8.0 1-33
Mobile IPv6 1-33
Benefits 1-33
Description 1-33
Supported Features 1-33
Session Continuity Support for 3GPP2 and WiMAX Handoffs 1-34
HA Features in Release 8.1 1-35
IP Services Gateway Features in Release 8.0 1-36
IP Services Gateway Features in Release 8.1 1-37
PDIF Features in Release 8.0 1-38
PDIF Features in Release 8.1 1-39
Congestion Control and Overload Disconnect Support 1-39
Custom DNS Handling 1-39
DELETE Payload Default Action Change 1-39
IPMS Support 1-40
Multiple Authentication 1-40
Online Upgrade 1-40
Public and Private Key Mismatch Check 1-40
Session Recovery 1-41
PDIF Features in Release 8.3 1-42
Multiple IPSec Traffic Selectors 1-42
Selective Diameter Profile Update Request Control 1-42
PDSN Features in Release 8.0 1-43
Traffic Shaping 1-43
PDSN Features in Release 8.1 1-44
Peer-to-Peer Features in Release 8.0 1-45
Peer-to-Peer Features in Release 8.1 1-46
P2P Protocols supported for detection 1-46
SGSN Features in Release 8.0 1-48
Limits / Engineering Rules 1-48
1-in-N IMEI Checks for Subscriber Events 1-48
1-in-N Selective Authentication of Subscriber Events 1-49
2.5G/3G Dual Access 1-49
Attach Rate Throttle 1-49
Fractional E1/DS1 Support 1-49
Disable Signaling Indication IE in RANAP messages 1-49
Ga Interface to the CGF/GSS 1-50
Gb-Flex - SGSN Pooling 1-50
Gs Interface to the MSC/VLR 1-51
Limiting Iu Connections in RANAP Messages 1-51

Local QoS Capping 1-51
Network-Initiated PDP Context Activation 1-52
QoS Traffic Policing per Subscriber 1-52
Session Recovery Support 1-52
Short Message Service - SMS 1-52
HSPA Fallback (aka Data Rate Management per RNC) 1-53
Tracking Usage of GPRS Encryption Algorithm 1-53
SGSN Behavior - Modified for Release 8.0 1-54
SGSN Features in Release 8.1 1-55
Default APN 1-55
Direct Tunnel Support 1-55
Disable Signaling Indication IE in RANAP messages 1-56
Ga Interface Supports Configurable Transport Layer 1-56
Hard Disk Storage for CDR Files 1-57
IuFlex / SGSN Pooling 1-57
Limiting Iu Connections in RANAP Messages 1-58
Local QoS Capping 1-58
Multiple PLMN Support (2.5G only) 1-58
Configuring Multiple PLMN Support: 1-58
Network Sharing 1-59
NPU FastPath 1-61
Quad Gig-E Line Card (QGLC) & Link Aggregation 1-62
Tracking Usage of GPRS Encryption Algorithm 1-62
Traffic Handling - QoS Provisioning with ARP 1-63
CLC2 - Channelized Line Card 2 1-63
OLC2 - Optical Line Card 2 1-63
Web Element Manager Features in Release 8.0 1-64
Support for Configurable DSCP Marking Based on Allocation/Retention Priority 1-64
Web Element Manager Path 1-64
Support for SGSN Bulk Statistics 1-64
Support for SGSN Alarms/Traps in Web Element Manager 1-65
Support for Content Filtering Report Configuration 1-66
Web Element Manager Path 1-66
Web Element Manager Features in Release 8.1 1-67
Support for PDIF functionality 1-67
Web Element Manager Path 1-67
Support for IKEv2 Transform Set 1-67
Web Element Manager Path 1-67
Support for Crypto Template 1-68
Web Element Manager Path 1-68
Support for IPv6 1-68
Web Element Manager Path 1-68
Support for Diameter Configuration 1-69
Web Element Manager Path 1-69
Support for URL Blacklisting Statistics 1-69
Web Element Manager Path 1-69

Support for Content Filtering Statistics 1-69
Web Element Manager Path 1-69
Support for EAP Profile 1-69
Web Element Manager Path 1-69
Support for Certificate Configuration 1-69
Web Element Manager Path 1-69
Support for Network Audit Tool 1-70
IPMP Configuration on WEM Server 1-70

Chapter 2: Fault Management

SNMP MIB Objects in Release 8.0 2-2
Modified Objects 2-2
Obsoleted Objects 2-3
New Objects 2-4
Deleted Objects 2-4
Modified Alarms 2-5
Obsoleted Alarms 2-5
New Alarms 2-6
Deleted Alarms 2-7
Web Element Manager Path 2-7
SNMP MIB Objects in Release 8.1 2-8
Modified Objects 2-8
Obsoleted Objects 2-9
New Objects 2-9
Deleted Objects 2-11
Modified Alarms 2-12
Obsoleted Alarms 2-13
New Alarms 2-13
Deleted Alarms 2-14
SNMP MIB Objects in Release 8.3 2-15
Modified Objects 2-15
Obsoleted Objects 2-15
New Objects 2-15
Deleted Objects 2-16
Obsoleted Alarms 2-16
New Alarms 2-16
Deleted Alarms 2-16
Content Filtering MIB Objects for Release 8.0 2-17
Modified Objects 2-17
Obsolete Objects 2-17
New Objects 2-17
Deleted Objects 2-17
Modified Alarms 2-17
Obsolete Alarms 2-18
New Alarms 2-18
Deleted Alarms 2-18

Web Element Manager Path 2-18
Content Filtering MIB Objects for Release 8.1 2-19
Modified Objects 2-19
Obsolete Objects 2-19
New Objects 2-19
Deleted Objects 2-19
Modified Alarms 2-19
Obsolete Alarms 2-19
New Alarms 2-19
Deleted Alarms 2-21
Content Filtering MIB Objects for Release 8.3 2-22
Modified Objects 2-22
Obsolete Objects 2-22
New Objects 2-22
Deleted Objects 2-22
Modified Alarms 2-22
Obsolete Alarms 2-22
New Alarms 2-22
Deleted Alarms 2-23
ESS MIB Objects for Release 8.0 2-24
Modified Objects 2-24
Obsolete Objects 2-24
New Objects 2-24
Deleted Objects 2-24
Modified Alarms 2-24
Obsolete Alarms 2-24
New Alarms 2-24
Deleted Alarms 2-24
ESS MIB Objects for Release 8.1 2-25
Modified Objects 2-25
Obsolete Objects 2-25
New Objects 2-25
Deleted Objects 2-25
Modified Alarms 2-25
Obsolete Alarms 2-25
New Alarms 2-26
Deleted Alarms 2-26
Intelligent Packet Monitoring Systems (IPMS) MIB in Release 8.1 2-27
New Objects 2-27
Modified Objects 2-27
Obsolete Objects 2-27
New Alarms 2-28
Modified Alarms 2-28
Obsolete Alarms 2-28
Web Element Manager Path 2-28
Web Element Manager Enhancements in Release 8.0 2-29

New Objects 2-29
Modified Objects 2-29
Obsolete Objects 2-29
New Alarms 2-29
Modified Alarms 2-29
Obsolete Alarms 2-29
Web Element Manager Path 2-29
Web Element Manager Enhancements in Release 8.1 2-30
New Objects 2-30
Modified Objects 2-30
Obsolete Objects 2-30
New Alarms 2-30
Modified Alarms 2-31
Obsolete Alarms 2-31
Web Element Manager Path 2-31

Chapter 3: Configuration Management

New Configuration Commands 3-2
Common Commands - New in Release 8.0 3-2
aaa accounting-overload-protection 3-2
alarm-disable 3-2
alarm-soak-timer 3-2
card smc upgrade 3-2
cdr 3-3
cdr-push 3-3
context-timeout 3-3
diameter send-ccri 3-4
flow-control 3-4
frame-relay 3-4
header-type 3-4
hopath-sdsf 3-5
hopath-sdsf 3-5
ingress-mode 3-5
initial-e1-framing 3-5
ipv6 access-list 3-5
line-timing 3-7
line-timing 3-7
link-aggregation 3-7
link-aggregation system-priority 3-8
loopback 3-8
lopath-sdsf 3-8
nai-construction 3-8
port bits 3-9
radius accounting interim volume 3-9
radius usage-reporting-algorithm 3-9
require detailed-rohc-stats 3-10

require diameter-proxy 3-10
show timing 3-10
toh-sdsf 3-10
This functionality is not supported at this time on the Web Element Manager. 3-10
use proxy 3-11
Common Commands - New in Release 8.1 3-12
card lc upgrade 3-12
cea-timeout 3-12
clear ipv6 neighbors 3-12
clock 3-13
diameter request-timeout 3-13
diameter sctp 3-13
dpa-timeout 3-13
flow-control 3-14
hd raid 3-14
hd raid 3-14
idle-timeout-activity ignore-downlink 3-14
ikev1 disable-phase1-rekey 3-15
ikev1 keepalive dpd 3-15
ikev1 policy 3-15
ipms 3-15
ping6 3-16
service-type 3-16
set control-dont-fragment 3-16
single-port-mode 3-17
tunnel selection-key 3-17
Common Commands - New in Release 8.3 3-18
diameter mscc-per-ccr-update 3-18
CF Commands - New in Release 8.0 3-19
failure-action 3-19
CF Commands - New in Release 8.1 3-20
content-filtering category match-method 3-20
content-filtering flow-any-error 3-20
discarded-flow-content-id 3-20
failure-action 3-20
upgrade url-blacklisting database 3-21
url-blacklisting action 3-21
url-blacklisting database 3-21
url-blacklisting match-method 3-21
ECS Commands - New in Release 8.0 3-22
add-ruledef 3-22
group-of-ruledefs 3-22
host-pool 3-22
http error 3-22
idle-timeout 3-23
imsi-pool 3-23

ip error 3-23
ip max-fragments 3-23
ip reset-tos 3-24
ip vlan 3-24
nexthop-forwarding-address 3-24
packet-filter 3-24
port-map 3-24
qos-class-identifier 3-25
qos-renegotiate traffic-class 3-25
qos-renegotiate timeout 3-25
rtcp uri 3-25
tcp check-window-size 3-26
tcp packets-out-of-order 3-26
tft packet-filter 3-26
url-extraction 3-26
wtp packets-out-of-order 3-26
ECS Commands - New in Release 8.1 3-28
bearer 3gpp apn 3-28
bearer 3gpp imsi 3-28
bearer 3gpp rat-type 3-28
bearer 3gpp sgsn-address 3-28
edr transaction-complete 3-29
extract-host-from-uri 3-29
http error 3-29
ip error 3-29
rtp parent-proto 3-30
rtcp parent-proto 3-30
start 3-30
tcp check-window-size 3-30
tcp mss 3-30
timedef 3-31
url-extraction 3-31
wsp x-header 3-31
ECS Commands - New in Release 8.3 3-32
post-processing priority 3-32
Firewall Commands - New in Release 8.0 3-33
firewall dos-protection 3-33
firewall flooding 3-33
firewall max-ip-packet-size 3-33
firewall mime-flood 3-33
firewall priority 3-34
firewall ruledef 3-34
firewall tcp-syn-flood-intercept 3-34
Firewall Commands - New in Release 8.1 3-35
bearer username 3-35
firewall flow-recovery 3-35

firewall icmp-destination-unreachable-message-threshold 3-35
firewall nat-alg 3-35
firewall no-ruledef-matches 3-36
firewall policy 3-36
firewall port-scan 3-36
firewall priority 3-36
firewall tcp-first-packet-non-syn 3-37
firewall tcp-idle-timeout-action 3-37
firewall track-list 3-37
flow any-error 3-37
nat policy 3-38
Firewall Commands - New in Release 8.3 3-39
firewall tcp-reset-message-threshold 3-39
GGSN Commands - New in Release 8.0 3-40
bearer-control-mode 3-40
gtpu udp-checksum insert 3-40
nai-construction 3-40
qos negotiate-limit 3-40
qos rate-limit 3-41
GGSN Commands - New in Release 8.1 3-42
clear gtpp storage-server local file statistics 3-42
credit-control-group 3-42
gtpp compression-process 3-42
gtpp dead-server suppress-cdrs 3-42
gtpp ram-disk-limit 3-43
gtpp secondary-group 3-43
gtpp storage-server local file 3-43
gtpp storage-server mode 3-43
gtpp storage-server mode 3-44
gtpp suppress-cdrs zero-volume-and-duration 3-44
gtpp transport-layer 3-44
GGSN Commands - New in Release 8.3 3-45
hd raid 3-45
HA Commands - New in Release 8.0 3-46
wimax-3gpp2 interworking 3-46
HA Commands - New in Release 8.1 3-47
delay interval 3-47
PDIF Commands - New in Release 8.0 3-48
PDIF Commands - New in Release 8.1 3-49
certificate 3-49
certificate 3-49
diameter authentication failure-handling 3-49
diameter disable endpoint 3-49
diameter enable endpoint 3-49
duplicate-session-detection 3-50
group 3-50

ignore-rekeying-requests 3-50
ikev2-ikesa 3-50
ip source-violation 3-51
ipv6 address 3-51
nai 3-51
radius accounting pdif trigger-policy 3-51
rekey 3-52
tsi start-address 3-52
PDSN Commands - New in Release 8.0 3-53
clear credit-control statistics 3-53
ipv6 router advertisement 3-53
mobile-ipv6 3-53
qos traffic-shape 3-53
policy ipv6 tunnel 3-54
PDSN Commands - New in Release 8.1 3-55
accounting trigger 3-55
ip routing overlap-pool 3-55
Session Control Manager Commands - New in Release 8.0 3-56
Session Control Manager Commands - New in Release 8.1 3-57
authorization 3-57
interface 3-57
nat-policy 3-57
plmn-id 3-57
policy 3-58
policy 3-58
sip-header 3-58
sip-param 3-58
SGSN Commands - New in Release 8.0 3-59
accept-procedure 3-59
accounting 3-59
accounting 3-59
associate-service 3-59
bssgp-timer 3-60
ciphering-algorithm 3-60
gmm information-in-messages 3-60
gmm retrieve-equipment-identity 3-60
gtp send 3-61
iu-recovery 3-61
llc 3-61
mtp2-lssu-len 3-61
network-initiated-pdp-activation 3-62
network-overload-protection 3-62
peer-network-service-entity 3-62
pool 3-62
rab-modify-procedure 3-63
ranap 3-63

re-authenticate 3-63
release-compliance 3-63
relocation-complete-timeout 3-64
reset-resource 3-64
resolver 3-64
retries 3-64
retry-count 3-64
sctp-max-out-strms 3-65
sctp-suppress-alarm 3-65
setup-timeout 3-65
sgsn-context-request 3-65
sgsn offload 3-66
sgsn imsimgr 3-66
short-message-service 3-66
sm 3-66
sm 3-67
threshold per-service-gprs-pdp-sessions 3-67
threshold per-service-gprs-sessions 3-67
threshold poll per-service-gprs-pdp-sessions interval 3-67
threshold poll total-gprs-pdp-sessions interval 3-67
threshold poll per-service-gprs-sessions interval 3-68
threshold poll total-gprs-sessions interval 3-68
threshold total-gprs-pdp-sessions 3-68
threshold total-gprs-sessions 3-68
timeout 3-68
timer 3-69
vlan-map 3-69
weight 3-69
SGSN Commands - New in Release 8.1 3-70
apn-selection-default 3-70
check-imei-timeout-action 3-70
clear gtpp storage-server local file statistics 3-70
clock-source 3-70
dns israu-mcc-mnc-encoding 3-71
gtpp compression-process 3-71
gtpp dead-server suppress-cdrs 3-71
gtpp ram-disk-limit 3-71
gtpp storage-server local file 3-72
gtpp storage-server mode 3-72
gtpp suppress-cdrs zero-volume-and-duration 3-72
gtpp transport-layer 3-72
inbound-asp-identifier validate 3-73
link-type 3-73
network-sharing cs-ps-coordination 3-73
ranap 3-73
ranap 3-74

reset-resource 3-74
routing-context 3-74
sgsn-number 3-74
super-charger 3-75
Modified Configuration Commands 3-76
Common Commands - Modified in Release 8.0 3-76
cca quota-state 3-76
clear subscriber sgsn-service 3-76
clock 3-76
congestion-control policy 3-77
diameter accounting 3-77
diameter authentication 3-77
diameter pending-timeout 3-78
failure-handling 3-78
failure-handling 3-78
file 3-79
file 3-79
frame-relay 3-80
lawful-intercept 3-80
logging filter runtime facility 3-80
newcall policy 3-82
ping 3-82
bind 3-82
Common Commands - Modified in Release 8.1 3-84
accounting trigger 3-84
attribute 3-84
attribute 3-84
bcmcs 3-85
cdr 3-85
clear crypto 3-85
framing 3-85
iiop port 3-86
ip access-list 3-86
ip pool 3-86
mobile-ip send 3-87
port-switch-on-l3-fail 3-87
radius accounting max-outstanding 3-87
radius charging accounting server 3-87
radius charging max-outstanding 3-88
radius charging server 3-88
radius max-outstanding 3-88
radius server 3-88
service-type 3-88
show srp 3-89
Common Commands - Modified in Release 8.3 3-90
attribute 3-90

ip pool 3-90
readdress server commands in inbound IPv4 ACLs 3-91
deny/permit (by TCP/UDP packets) 3-92
threshold cpu-orbs-warn 3-92
threshold cpu-orbs-crit 3-92
CF Commands - Modified in Release 8.0 3-93
analyze 3-93
analyze 3-93
CF Commands - Modified in Release 8.1 3-94
analyze 3-94
content-filtering 3-95
content-filtering category policy-id 3-95
timeout action 3-95
ECS Commands - Modified in Release 8.0 3-96
action 3-96
bearer imsi 3-96
charge-volume 3-96
charging-rule-optimization 3-97
dictionary 3-97
flow action 3-97
flow limit-across-applications 3-98
flow limit-for-bandwidth 3-98
ip dst-address 3-98
ip server-ip-address 3-98
ip src-address 3-99
ip subscriber-ip-address 3-99
ip tos 3-99
mms bcc 3-100
mms cc 3-100
mms content location 3-100
mms content type 3-100
mms from 3-100
mms message-id 3-101
mms subject 3-101
mms to 3-101
p2p protocol 3-101
p2p detection-protocol 3-102
ruledef 3-103
rule-variable 3-103
tcp either-port 3-103
tcp dst-port 3-104
tcp src-port 3-104
udp dst-port 3-104
udp either-port 3-104
udp src-port 3-105
license 3-105

ECS Commands - Modified in Release 8.1 3-106
action priority 3-106
attribute 3-106
credit-control 3-107
flow action 3-107
flow action redirect-url 3-107
flow limit-for-bandwidth 3-107
icap server 3-108
insert 3-108
ip protocol 3-109
ip tos 3-109
ping6 3-109
p2p protocol 3-110
p2p detection-protocol 3-110
require active-charging 3-111
rule-variable 3-112
ECS Commands - Modified in Release 8.3 3-113
file sequence-number 3-113
require active-charging 3-113
rule-application 3-114
Firewall Commands - Modified in Release 8.0 3-115
firewall policy 3-115
firewall policy 3-115
Firewall Commands - Modified in Release 8.1 3-115
firewall dos-protection 3-115
firewall flooding 3-116
firewall icmp-destination-unreachable-message-threshold 3-116
firewall max-ip-packet-size 3-116
firewall mime-flood 3-117
firewall no-ruledef-matches 3-117
firewall priority 3-117
firewall tcp-syn-flood-intercept 3-118
ip protocol 3-118
Firewall Commands - Modified in Release 8.3 3-119
firewall no-ruledef-matches 3-119
firewall priority 3-119
GGSN Commands - Modified in Release 8.0 3-120
allow aaa-assigned-hostname 3-120
bearer-control-mode 3-120
cc profile 3-120
gtpp dictionary 3-120
gtpp error-response 3-121
gtpp interim now 3-121
gtpp max-cdrs 3-121
sgsn-address 3-122
GGSN Commands - Modified in Release 8.1 3-123

gtpp dictionary 3-123
gtpp egcdr 3-123
gtpu udp-checksum insert 3-123
gtpp storage-server local file 3-124
qos rate-limit { downlink | uplink } 3-124
ipv6 pool 3-124
tunnel l2tp 3-125
HA Commands - Modified in Release 8.0 3-126
authentication aaa-distributed-mip-keys 3-126
HA Commands - Modified in Release 8.1 3-127
redirect 3-127
NAT Commands - Modified in Release 8.3 3-128
nat policy 3-128
PDIF Commands - Modified in Release 8.0 3-129
PDIF Commands - Modified in Release 8.1 3-130
aaa attribute 3-130
aaa authentication 3-130
authentication 3-130
group 3-131
hmac 3-131
IKEv2-IKESA policy error notification 3-131
peer 3-131
proxy-mip 3-132
server 3-132
PDSN Commands - Modified for Release 8.0 3-133
file 3-133
PDSN Commands - Modified for Release 8.1 3-134
ipv6 pool 3-134
ink aggregation 3-134
clear snmp trap 3-134
PDSN Commands - Modified for Release 8.3 3-135
bcmcs 3-135
Session Control Manager Commands - Modified for Release 8.0 3-136
Session Control Manager Commands - Modified for Release 8.1 3-137
access-type 3-137
cnsa-media-profile 3-137
This functionality is not supported at this time on the Web Element Manager. 3-137
diameter 3-137
policy 3-138
trusted-domain-entity 3-138
SGSN Commands - Modified for Release 8.0 3-139
accounting 3-139
accounting 3-139
application-context-name 3-139
authenticate all-event 3-139
authenticate attach 3-140

authenticate frequency 3-140
authenticate rau update-type 3-140
bind link 3-141
cc profile 3-141
ciphering-algorithm 3-141
clear subscriber 3-141
equipment-identity-register 3-142
frame-relay 3-142
gmm 3-142
gmm 3-143
gtpp 3-143
gtpp dictionary 3-144
gtpp interim now 3-144
gtpp max-cdrs 3-144
gtpp trigger 3-145
lawful-intercept 3-145
lawful-intercept 3-145
llc 3-146
llc 3-146
llc 3-147
llc 3-147
map 3-147
network-service-entity ip 3-147
network-service-entity 3-147
network-service-entity ip-local 3-148
nri 3-148
ns-timer 3-149
ns-vc 3-149
nsvl 3-149
nsvl-address 3-149
paging-policy 3-150
paging-policy 3-150
partial-apn-match 3-150
peer-nsei 3-150
qos class 3-151
qos class 3-151
qos prefer-as-cap 3-151
rau-inter 3-152
requested-apn-from-first-subrec 3-152
sgsn-context-request 3-152
show session 3-152
sm 3-153
trim-trailing-spaces-in-apn 3-153
SGSN Commands - Modified for Release 8.1 3-154
apn/apn-selection-default/wildcard-apn 3-154
authenticate rau update-type 3-154

frame-relay 3-154
gtpp storage-server local file 3-154
gtpc 3-155
imsi 3-155
imsi 3-155
llc 3-156
nri length 3-156
qos prefer-as-cap 3-157
qos rate-limit 3-157
radio-network-controller 3-157
ranap allocation-retention-priority-ie 3-158
routing-context 3-158
Obsoleted Commands 3-159
Common Commands - Obsoleted in Release 8.0 3-159
context-cleanup-period 3-159
diameter dictionary 3-159
fragment-size 3-159
header-type 3-159
service-type 3-160
tx-priority 3-160
vc-mapping 3-160
{ deny | permit } [log] { tcp | udp } 3-160
Common Commands - Obsoleted in Release 8.1 3-161
enable/disable super-charger 3-161
isakmp disable-phase1-rekey 3-161
isakmp keepalive 3-161
isakmp policy 3-161
CF Commands - Obsoleted in Release 8.0 3-162
timeout action 3-162
CF Commands - Obsoleted in Release 8.1 3-163
timeout action 3-163
ECS Commands - Obsoleted in Release 8.0 3-164
tcp out-of-order-timeout 3-164
wtp out-of-order-timeout 3-164
ECS Commands - Obsoleted in Release 8.1 3-165
bearer apn 3-165
bearer imsi 3-165
bearer rat-type 3-165
bearer sgsn-address 3-165
Firewall Commands - Obsoleted in Release 8.0 3-166
Firewall Commands - Obsoleted in Release 8.1 3-167
firewall policy 3-167
GGSN Commands - Obsoleted in Release 8.0 3-168
qos traffic-policing 3-168
qos-renegotiation 3-168
timeout 3-168

GGSN Commands - Obsoleted in Release 8.1 3-169
HA Commands - Obsoleted in Release 8.0 3-170
HA Commands - Obsoleted in Release 8.1 3-171
PDSN Commands - Obsoleted in Release 8.0 3-172
PDSN Commands - Obsoleted in Release 8.1 3-173
Session Control Manager Commands - Obsoleted in Release 8.0 3-174
Session Control Manager Commands - Obsoleted in Release 8.1 3-175
access-network 3-175
SGSN Commands - Obsoleted in Release 8.0 3-176
Gs Service Configuration Mode 3-176
NSE-FR Configuration Mode 3-176
NSE-IP Configuration Mode 3-176
SGSN Operator Policy Configuration Mode 3-176
SGSN Service Configuration Mode 3-176
SGSN Commands - Obsoleted in Release 8.1 3-177
GTPP Storage Server (GSS) 3-178
GSS Changes in Release 8.0 3-178
GSS Changes in Release 8.1 3-178
Web Element Manager Changes 3-179

Chapter 4: Accounting Management

Bulk Statistic Enhancements in Release 8.0 4-2
Bulk Statistic Additions 4-2
Context Schema 4-2
gprs schema 4-2
gtpc schema 4-3
gtpp schema 4-4
sccp schema 4-4
sgsn schema 4-4
sgtp schema 4-25
ss7link schema 4-27
ss7rd schema 4-27
system schema 4-28
Bulk Statistic Modifications 4-34
Obsoleted Bulk Statistics 4-34
gprs schema 4-34
sgsn schema 4-35
sgtp schema 4-37
Web Element Manager Path 4-37
Bulk Statistic Enhancements in Release 8.1 4-38
Bulk Statistic Additions 4-38
ECS Schema 4-38
Card Schema 4-39
System Schema 4-40
Port Schema 4-42
GPRS Schema 4-43

GTPC Schema 4-43
GTPC Schema 4-44
System Schema 4-44
SGSN Schema 4-44
CSCF Schema 4-44
CSCFINTF Schema 4-58
Obsoleted Bulk Statistics 4-59
GTPP Schema 4-59
System Schema 4-59
HAMIPv6 Schema 4-61
Obsoleted Bulk Statistics 4-62
HAMIPv6 Schema 4-62
Bulk Statistic Enhancements in Release 8.3 4-63
Bulk Statistic Additions 4-63
nat-realm Schema 4-63
system Schema 4-63
PDIF schema 4-69
CDR Enhancements 4-70
Command Enhancements 4-71
New Commands 4-72
Diameter AVPs in Release 8.0 4-73
New Attributes 4-73
Modified Attributes 4-75
Removed Attributes 4-75
Diameter AVPs in Release 8.1 4-76
New Attributes 4-76
Modified Attributes 4-77
Removed Attributes 4-77
RADIUS Attributes in Release 8.0 4-78
New Attributes 4-78
Modified Attributes 4-79
Removed Attributes 4-79
RADIUS Attributes in Release 8.1 4-80
New Attributes 4-80
Modified Attributes 4-80
Removed Attributes 4-81
RADIUS Attributes in Release 8.3 4-82
New Attributes 4-82
Modified Attributes 4-82
Removed Attributes 4-82
Web Element Manager Enhancements 4-83

Chapter 5: Performance Management

New Commands 5-2
Common Commands - New in Release 8.0 5-2
show diameter message-queue 5-2

show multicast-sessions all 5-2
dns-client 5-2
Common Commands - New in Release 8.1 5-3
show hd raid 5-3
show ipv6 interface summary 5-3
show ipv6 neighbor 5-3
show ipv6 route 5-3
show port info 5-3
show port table 5-4
show subscribers 5-4
show configuration errors 5-4
show ipms status 5-5
Common Commands - New in Release 8.3 5-6
clear radius accounting archive 5-6
CF Commands - New in Release 8.0 5-7
clear content-filtering category statistics 5-7
CF Commands - New in Release 8.1 5-8
clear active-charging url-blacklisting statistics 5-8
show active-charging content-filtering category policy-id 5-8
show active-charging url-blacklisting statistics 5-8
show url-blacklisting database 5-8
show url-blacklisting url 5-9
ECS Commands - New in Release 8.0 5-10
clear active-charging group-of-ruledefs statistics 5-10
show active-charging group-of-ruledefs 5-10
show active-charging packet-filter 5-10
ECS Commands - New in Release 8.1 5-11
show active-charging timedef 5-11
Firewall Commands - New in Release 8.0 5-12
clear active-charging firewall statistics 5-12
show active-charging firewall statistics 5-12
threshold fw-deny-rule 5-12
threshold fw-dos-attack 5-12
threshold fw-drop-packet 5-13
threshold fw-no-rule 5-13
Firewall Commands - New in Release 8.1 5-14
clear active-charging firewall track-list 5-14
show active-charging firewall track-list 5-14
GGSN Commands - New in Release 8.0 5-15
show gtpp group 5-15
GGSN Commands - New in Release 8.1 5-16
show mbms bearer-service 5-16
show gtpp storage-server 5-16
HA Commands - New in Release 8.0 5-17
HA Commands - New in Release 8.1 5-18
NAT Commands - New in Release 8.3 5-19

clear active-charging nat statistics 5-19
nat-realm schema 5-19
show active-charging nat statistics 5-19
show bulkstats variables nat-realm 5-19
threshold nat-port-chunks-usage 5-20
threshold poll nat-port-chunks-usage 5-20
snmp trap { enable | suppress } ThreshClearNATPortChunksUsage 5-20
snmp trap { enable | suppress } ThreshNATPortChunksUsage 5-20
PDIF Commands - New in Release 8.0 5-21
PDIF Commands - New in Release 8.1 5-22
show certificate 5-22
show crypto ikev2-ikesa security-associations summary table 5-22
show crypto managers instance 5-22
show crypto managers summary 5-22
show crypto statistics ikev2 5-22
PDSN Commands - New in Release 8.0 5-24
show credit-control session 5-24
show credit-control statistics 5-24
PDSN Commands - New in Release 8.1 5-25
SGSN Commands - New in Release 8.0 5-26
show network-service-entity 5-26
show sgsn-operator-policy full 5-26
SGSN Commands - New in Release 8.1 5-27
clear super-charger 5-27
show freeze-ptmsi 5-27
show super-charger 5-27
Modified Commands 5-28
Common Commands - Modified in Release 8.0 5-28
clear cscf-service 5-28
clear subscribers 5-28
clear subscribers gtp-version 5-28
monitor subscriber type 5-28
show aaa 5-29
show cscf-service 5-29
show radius counters all 5-29
show session subsystem facility aaamgr all 5-30
show subscribers 5-30
show subscribers 5-30
show subscribers full 5-31
show subscribers gtp-version 5-31
threshold monitoring 5-31
threshold poll 5-31
show port table 5-32
Common Commands - Modified in Release 8.1 5-33
clear subscribers 5-33
show dhcp-service name 5-33

show diameter aaa-statistics 5-33
show diameter authentication servers 5-34
show diameter peers full all 5-34
show ims-authorization policy-control statistics 5-34
show ims-authorization sessions full 5-35
show resources 5-35
show session subsystem facility sessmgr all 5-36
show subscribers 5-36
show subscribers full 5-36
Common Commands - Modified in Release 8.3 5-37
clear subscribers 5-37
show subscribers 5-37
show subscribers full 5-37
CF Commands - Modified in Release 8.0 5-38
show active-charging content-filtering category statistics 5-38
show active-charging content-filtering server-group 5-38
show content-filtering category database 5-38
show content-filtering category statistics 5-39
show content-filtering category statistics 5-39
CF Commands - Modified in Release 8.1 5-40
show active-charging content-filtering category policy-id 5-40
show active-charging content-filtering category statistics verbose 5-40
show active-charging content-filtering server-group 5-40
show active-charging service name 5-40
show content-filtering category database 5-41
show content-filtering category policy-id 5-41
show content-filtering category statistics facility srdbmgr instance 5-41
ECS Commands - Modified in Release 8.0 5-42
show active-charging analyzer statistics name ip verbose 5-42
show active-charging charging-action name 5-42
show active-charging charging-action statistics 5-42
show active-charging content-filtering server-group statistics 5-43
show active-charging edr-udr-file statistics 5-43
show active-charging ruledef 5-43
clear active-charging ruledef statistics 5-44
show active-charging sessions 5-44
show active-charging sessions full 5-44
show active-charging sessions full all 5-45
show active-charging subsystem 5-45
show port info 5-45
ECS Commands - Modified in Release 8.1 5-47
clear active-charging analyzer statistics 5-47
clear active-charging credit-control statistics 5-47
show active-charging analyzer statistics name p2p 5-48
show active-charging charging-action all 5-48
show active-charging credit-control statistics 5-49

show active-charging flows 5-49
show active-charging flows full 5-50
show active-charging rulebase name 5-50
show active-charging rulebase statistics 5-52
show active-charging service 5-52
show active-charging sessions 5-53
show active-charging sessions 5-54
show active-charging subsystem 5-55
show active-charging subsystem facility acsmgr instance 5-55
ECS Commands - Modified in Release 8.3 5-56
show active-charging edr-format statistics 5-56
show active-charging charging-action statistics name 5-56
show active-charging flows 5-57
show active-charging ruledef 5-57
show active-charging rulebase name 5-58
show active-charging rulebase statistics 5-58
show active-charging rulebase statistics name 5-58
show active-charging sessions full all 5-58
show active-charging subsystem all 5-59
Firewall Commands - Modified in Release 8.1 5-60
clear active-charging firewall statistics 5-60
show active-charging firewall statistics 5-60
GGSN Commands - Modified in Release 8.0 5-61
show apn statistics name 5-61
show gtpc full 5-61
show gtpc statistics verbose 5-61
show gtpc statistics verbose 5-62
show gtpp counters all 5-62
show gtpp statistics cgf-address 5-62
GGSN Commands - Modified in Release 8.1 5-63
show gtpp storage-server 5-63
show subscriber ggsn-only 5-63
show apn name 5-63
show subscribers 5-64
show gtpc statistics 5-64
clear gtpc statistics 5-64
show apn statistics 5-64
show apn all 5-65
show subscribers ggsn-only 5-65
HA Commands - Modified in Release 8.0 5-67
HA Commands - Modified in Release 8.1 5-68
PDIF Commands - Modified in Release 8.0 5-69
PDIF Commands - Modified in Release 8.1 5-70
show crypto statistics ikev2 5-70
show crypto managers instance 5-70
show crypto map 5-70

show session subsystem facility aaamgr all 5-71
show crypto ipsec security-associations 5-71
PDIF Commands - Modified in Release 8.3 5-72
show crypto transform-set 5-72
show pdif-service statistics 5-72
PDSN Commands - Modified in Release 8.0 5-73
PDSN Commands - Modified in Release 8.1 5-74
show hd raid verbose 5-74
Session Control Manager Commands - Modified for Release 8.0 5-75
Session Control Manager Commands - Modified for Release 8.1 5-76
clear cscf service 5-76
clear cscf sessions 5-76
clear cscf sip 5-76
show cscf service 5-76
show cscf sessions 5-77
show cscf sip 5-77
show cscf tcp connections 5-77
SGSN Commands - Modified in Release 8.0 5-78
show dns-client 5-78
show gmm-sm statistics 5-78
show gmm-sm statistics 5-79
show gmm-sm statistics 5-79
show gmm-sm statistics 5-79
show gtpp counters all 5-87
show gtpp storage-server 5-88
show gtpp storage-server statistics 5-89
show iups-service 5-89
show sccp-network 5-89
show session disconnect-reasons verbose 5-90
show session subsystem 5-90
show sgtp-service 5-90
show ss7-routing-domain 5-91
show ss7-routing-domain 5-91
show subscriber 5-91
show subscriber 5-92
show sgtpu statistics 5-92
show llc statistics 5-92
show sndcp statistics verbose 5-93
show sgtpu statistics 5-93
show sgtpu statistics 5-94
show gprs-service all 5-94
show gprs-service all 5-94
show gmm-sm statistics 5-94
show gprs-service all 5-95
SGSN Commands - Modified in Release 8.1 5-96
clear sgtpu-statistics 5-96

show gmm-sm statistics 5-96
show gmm-sm statistics verbose 5-96
show iups-service 5-97
show sgtpu-statistics 5-97
show gmm-sm statistics 5-97
show gmm-sm statistics 5-98
show gmm-sm statistics verbose 5-98
show subscribers sgsn-only full 5-99
show sgtpu statistics 5-99
show gmm-sm statistics verbose 5-99
Obsoleted Commands 5-101
Common Commands - Obsoleted from Release 8.0 5-101
Common Commands - Obsoleted from Release 8.1 5-101
CF Commands - Obsoleted from Release 8.0 5-102
CF Commands - Obsoleted from Release 8.1 5-102
show content-filtering category policy-id 5-102
ECS Commands - Obsoleted from Release 8.0 5-103
ECS Commands - Obsoleted from Release 8.1 5-103
Firewall Commands - Obsoleted from Release 8.0 5-104
clear firewall flows 5-104
clear firewall ruledef 5-104
clear firewall statistics 5-104
show firewall flows 5-104
show firewall ruledef 5-105
show firewall statistics 5-105
update firewall policy 5-105
Firewall Commands Obsoleted from Release 8.1 5-105
GGSN Commands - Obsoleted from Release 8.0 5-106
GGSN Commands - Obsoleted from Release 8.1 5-106
HA Commands - Obsoleted from Release 8.0 5-107
HA Commands - Obsoleted from Release 8.1 5-107
PDSN Commands - Obsoleted from Release 8.0 5-108
PDSN Commands - Obsoleted from Release 8.1 5-108
SGSN Commands - Obsoleted from Release 8.0 5-109
SGSN Commands - Obsoleted from Release 8.1 5-109
GTPP Storage Server Changes 5-110
Web Element Manager Changes 5-111

Chapter 6: Security Management

Security Enhancements 6-2
New Commands 6-2
cli login-failure-delay 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 7.x and 8.x. All features listed in this guide are split up according to the release that it was initially supported in.

Additional information on the new features is available in the following documents:

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
Content Filtering Services Administration Guide	901-00-0056 I
Peer-to-Peer Detection Administration Guide	901-00-0057 K
Packet Data Interworking Function Administration Guide	901-00-0059 J
Personal Stateful Firewall Administration Guide	901-00-0060 L
ST16 Hardware Installation and Administration Buide	901-00-0088 A

Common Features in Release 8.0

This section provides information on new features that are common to all products in Release 8.0.

Configurable Transmit Timing Source

It is now possible to configure the transmit clock source, as either Building Integrated Timing Supply (BITS) or line-timing, for application services using SDH or SONET over the Optical line card or the Channelized line card.

BITS-timing provides the transmit timing source, using Stratum 3 compliant BITS modules resident on either the SPIO with a BITS BNC interface or the SPIO with a BITS 3-pin interface. Line-timing recovers the receive timing from an external clock source via a port on an Optical or Channelized line card. It is possible to configure both clock sources, so that one timing source backs up the other.

To configure and manage this feature, a new CLI configuration sub-mode has been added to the Global configuration mode - the BITS Port Configuration Mode, details in the *Command Line Interface Reference*, includes the following new commands:

- default
- end
- exit
- mode
- preferred slot
- recover
- shutdown
- snmp trap link-status

Configuration of this clock source is explained in *Configuring Transmit Timing Source* in the *System Administration Guide*.

CDR PUSH Transfer Mode

The CDR files can be pushed from the chassis to the configured external storage server periodically using the SFTP protocol. This functionality is supported both on the ST16 and ST40 platforms.

With the PUSH transfer mode, the external storage server URL to which the CDR files need to be transferred should be specified. The configuration allows a primary and a secondary server to be configured. Configuring the secondary server is optional. Whenever a file transfer to the primary server fails for four consecutive times, the files will be transferred to the secondary server. The transfer will switch back to the original primary server when:

- Four consecutive transfer failures to the secondary server occur
- After switching from the primary server, 30 minutes elapses

With the push transfer mode, the following can be configured:

- Transfer interval: A time interval, in seconds, after which the CDRs are pushed to the configured IP periodically. All the files that are completed before the PUSH timer expires are pushed.
- Remove file after transfer: An option to keep or remove the CDR files on the hard disk after they are transferred to the external storage server successfully.

DHCP Service Support with MPLS Labels

This support added to configure traffic from the specified DHCP service bind address to use the MPLS labels. This support also provides the configuration to define the next-hop gateway address.

To configure and manage this feature, a new optional keyword **`nexthop-forwarding-address`** *`nexthop_ip_address`* with other options has been added to the **`bind address`** *`ip_address`* command in DHCP Configuration mode in the *Command Line Interface Reference*.

Configuration of this support is explained in *Multi Protocol Label Switching* chapter in the *System Enhanced Feature Configuration Guide*.

IMPORTANT

To enable this feature you need MPLS feature license on your system.

Four-Port Gigabit Ethernet Line Card (QGLC)

A new four port Gigabit Ethernet line card (usually referred to as the Quad Gig-E Line Card or QGLC) has been introduced for the ST40 platform only.

Using hot-swappable small form-factor pluggable (SFP) modules, the card can support either 1000Base-SX, 1000base-LX and 1000Base-T configurations. Note that all four ports must be of one type; there can be no mix-and-matching interfaces.

QGLCs can be installed in chassis slots 17 through 23, 26 through 39, and 42 through 48. These cards should always be installed directly behind their respective PSCs, but are not required to be placed behind any redundant PSCs (those operating in Standby mode). Cards inserted in pairs behind an active PSC offer 1:1 redundancy and automatic failover.

It has four ports instead of one which is less expensive than having to buy more than one line card if you need more than one port. With more ports the QGLC line card increases aggregate throughput to external devices (up to 2.8 Gbps depending on call model).

The QGLC uses a new generation of Fixed Programmable Gate Array (FPGA).The new FPGA allows the Star Channel (the 140Gbps internal bus) to be used for firmware upgrades. This dramatically improves the time it takes upgrade the card firmware for future enhancements.

See also the “Link Aggregation” section below.

For more information, see the “Hardware Platform Overview” chapter of the *Hardware Installation and Administration Guide*.

Hard Disk Support on SMC Card in ST40 Platform

To add storage capability a hard disk drive (HDD) has been introduced in the ST40 platform.

When storing CDR files on the SMC HDD, at first they are stored on the RAMFS before being moved to the HDD. The files can then be off-loaded via FTP or SFTP to an external server (such as the L-ESS or the GSS) or billing system.

When using the HDD for EDR/UDR storage, EDR/UDR files are transferred from RAMFS on the PSC card to the HDD on the SMC card. The HDD may also be used to store any data that needs to be backed up.

The secondary SMC card also contains an HDD, which serves as a redundant and becomes active during an SMC failover. The HDD on the secondary is mirrored to the HDD on the primary in order to avoid any data loss. Basically, the drives are raid-1 redundant.

HDD support is only available on the ST40 platform, so in the case of an “ST16” or an “ST40 without a HDD”, a card failover results in a loss of CDR files. In the case of card failover on an “ST40 with a HDD”, the new Active SMC starts pushing the files. Any files that are left in the middle of the transfer will be transferred again.

“monitor protocol” CLI Command Option to use with HDD Configuration

If the hard disk drive (HDD) is used for CDR storage, with the **`monitor protocol`** CLI command in the Exec Mode, the CDR option (29) must be used and not GTPP option (27).

Link Aggregation

Provides a means of aggregating or trunking from one to four ports on a redundant pair of Quad Gig-E line cards (QGLC) in order to guarantee a file transmission is sent serially over one link until it is finished downloading. Each PSC and its associated QGLC(s) forms a system and negotiates with an aggregation on a remote port using Link Aggregation Configuration Protocol (LACP).

For more information see “Configuring System Options” in the *System Administration Guide*.

New SNMP MIB Objects and Traps

This release supports many new SNMP MIB objects and traps as indicated in this guide.

New Bulk Statistics

This release supports many new bulk statistics as indicated in this guide.

New RADIUS Attributes

This release supports many new RADIUS attributes as indicated in this guide.

Configuration and Performance Parameter Enhancements

This release includes a number of new and/or modified commands and Web Element Manager application functions. These are detailed in this guide.

Software Patch Upgrades Not Supported

Software Patch Upgrades are not supported in this release.

Common Features in Release 8.1

This section provides information on new features that are common to products in Release 8.1.

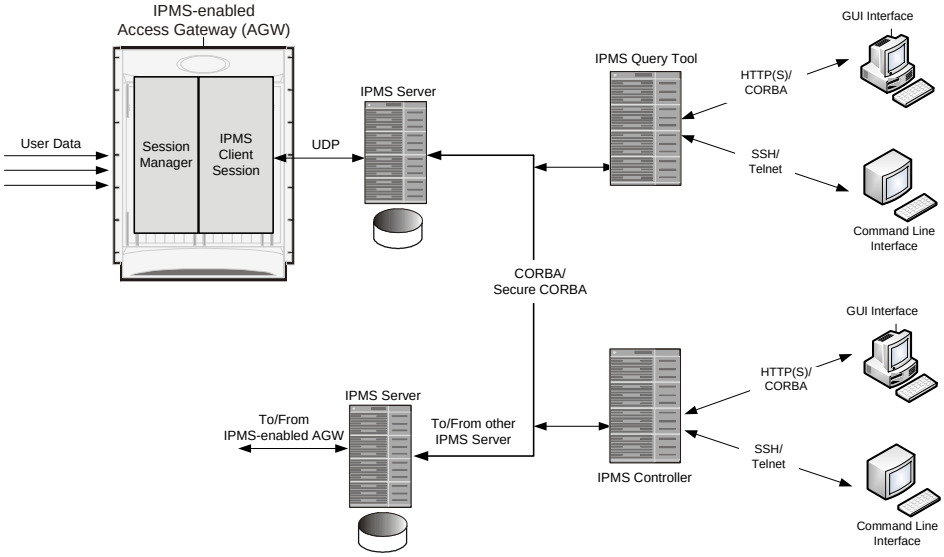
Duplicate CDR Detection

When AAA proxy is configured to write CDRs into the SMC hard disk, there are chances of duplicate records being written to the file if the AAA proxy crashes after writing the file to the RAM disk and before sending an ACK to AAAMgr. To prevent this, a mechanism is now in place for the AAA proxy to avoid writing duplicate records when AAAMgr retransmits the request later.

Intelligent Packet Monitoring System (IPMS)

The Starent Networks now provides IPMS (Intelligent Packet Monitoring System) solution for operators to analyze and investigate call related events on the Starent Networks Access Gateways (AGWs) like PDIF, PDSN, GGSN, SGSN, etc.

The Intelligent Packet Monitoring System application provides the functions to assist operators to analyze and investigate call related events at a later point of time. When IPMS is enabled for a product, the AGW sends a copy of call control events as well as system event packets (IKE, Proxy-MIP, RADIUS, DIAMETER etc.) with some additional information to an external server for every call as part of normal system processing. The external server stores the received call control events and system event packets for later analysis.



IMPORTANT

Initially IPMS is available for Starent Networks PDIF access gateway only.

The IPMS client service can be enabled on AGW through **ipms** command in Context Configuration Mode and IPMS servers can be configured in IPMS Client Configuration Mode on an AGW. For more information on hardware and other requirements for this application support, refer *IPMS Installation and Administration Guide*.

The Intelligent Packet Monitoring System solution is a separate product and must be purchased separately. Contact your designated sales or service representative.

Domain-based L2TP Tunnel Support

This feature enables initiation of new L2TP create tunnel request to same LNS address based on the value of attribute “Tunnel-Server-Auth-ID” in *Access-Accept* message received from AAA server. This value is treated as a key to identify tunnel. Thus, effectively, this result in multiple L2TP tunnels based on the value of attribute received from AAA server by a LAC. This value of attribute is treated as a key to identify tunnel.

In earlier implementation, LAC chooses to create a new tunnel between LAC and LNS pair only when existing tunnel has reached its full capacity of allowed L2TP sessions per tunnel. There was no provision to the further segregation of the traffic between LAC and LNS.

New CLI command **tunnel selection-key { tunnel-server-auth-id | none }** is added in LAC service configuration mode to support this feature. This command will provide facility to create new tunnel on the basis of value of domain attribute received from AAA server before reaching the session capacity on existing tunnels.

IMPORTANT

Currently this support is available for GGSN only.

Software Patch Upgrades Not Supported

Software Patch Upgrades are not supported in this release.

Common Features in Release 8.3

This section provides information on new features that are common to all products in Release 8.3.

Packet Services Card 2

The Packet Services Card 2 (PSC2) is the next-generation packet forwarding card for the ST40. The PSC2 provides increased aggregate throughput and performance, and a higher number of subscriber sessions.

The PSC2 has been enhanced with a faster network processor unit, featuring two quad-core Intel x86 2.5Ghz CPUs, 32 GB of RAM. The PSC2 provides 2 to 2.7 times the data throughput of the original PSC, and the switch fabric interface has been doubled.

A second-generation data transport fixed programmable gate array (DT2 FPGA, abbreviated as DT2) connects the PSC2'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 PSC2 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.

Interoperability

It is not recommended that PSC2s are mixed with PSCs, since this prevents the PSC2 from operating at its full potential. Due to the different processor speeds and memory configurations, the PSC2 cannot be combined in a chassis with the original PSC 16 GB.

For more information, see the "Hardware Platform Overview" chapter of the *Hardware Installation and Administration Guide*.

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.

The XGLC is a full-height line card. To install an XGLC, you must remove the half-height card guide in the rear of the chassis. Once installed, use only the upper slot number to refer to or configure the XGLC. XGLCs can be installed in chassis slots 17 through 23 and 26 through 32. These cards should always be installed directly behind their respective PSCs or PSC2s, but they are not required behind any redundant PSCs or PSC2s (those operating in Standby mode).

The one-port XGLC supports the IEEE 802.3-2005 revision which defines full duplex operation of 10 Gigabit Ethernet.

The XGLC use a Small Form Factor Pluggable (SPF+) module. The modules support one of two media types: 10GBASE-SR (Short Reach) 850nm, 300m over Multimode (MMF), or 10GBASE-LR (Long Reach) 1310nm, 10km over Single Mode (SMF).

The XGLC is configured and monitored via the System Management Card (SMC) over the system's control bus. Both SMCs must be active to maintain maximum forwarding rates.

A feature of the higher speed line cards (XGLC and the Quad Gigabit Ethernet Line Card or QGLC), is the ability to use the Star Channel if the firmware needs to be upgraded. The Star Channel is a 2x140Gbps redundancy bus between the PSC and the line card that allows a faster download. Another way to perform a firmware upgrade is via the System Management Bus, with 1 Mbps throughput, which connects the SMC to every card in the system.

The supported redundancy scheme for XGLC is L3, Equal Cost Multi Path (ECMP).

For more information, see the "Hardware Platform Overview" chapter of the *Hardware Installation and Administration Guide*.

ASN GW Features in Release 8.0

This section provides information for new features in the ASN GW Service in Release 8.0.

Currently, there are no new ASN GW features in Release 8.0.

ASN GW Features in Release 8.1

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

IMPORTANT

The features in this section are all available in Release 8.1

Multi-host Support

ASN GW now supports multi host feature to provide multiple host connectivity.

The WiMAX CPE modem is used in Fixed/Nomadic application to support multiple IP hosts and it share the singles WiMAX airlink to connect to the WiMAX IP network.

This feature is a effective solution for Small Office/Home Office (SOHO) users to provide multiple station connectivity through one airlink.

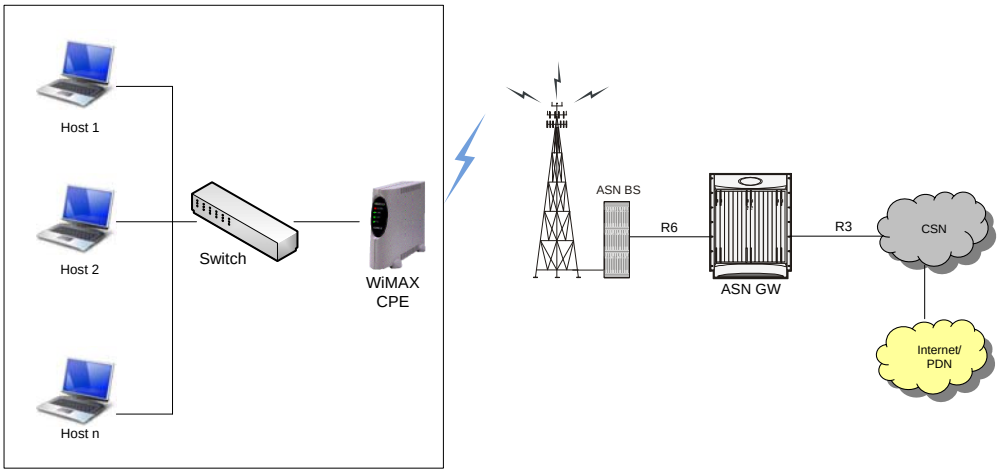


Figure 1-1 Multi Host Support with WiMAX Network

The WiMAX ASNGW allows each WiMAX MS (identified by its 6-byte MSID) to be assigned with a single IP address. IP accounting is maintained for the IP address.

The ASNGW is responsible for managing the allocation and freeing of IP address, to manage the data path for it and to maintain accounting of data packets for it.

For more information on this feature, refer to the *Multi-host Support* section in *ASN GW Overview* chapter.

Content Filtering in Release 8.0

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

Currently, there are no new Content Filtering features in Release 8.0

Content Filtering in Release 8.1

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

IMPORTANT

The new features in this section are all available in Release 8.1.

URL Blacklisted Content Filtering

In the URL Blacklisted Content Filtering solution, all HTTP/WAP requests from subscribers are inspected in order to determine the requested destination URLs/URIs. Each URL/URI is then matched against a database of blacklisted URLs, if there is a match, one fixed action—discard, redirect, or terminate—is taken. If the requested URL/URI is not present in the blacklist in its exact, literal form then the request is passed on as usual. This content filtering solution can either be applied to all subscribers or none. Typical cases include applying a blacklisted database of child porn URLs to all subscribers so that they are not inadvertently exposed to such content.

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

ECS Features in Release 8.0

This section provides information for new features in the Enhanced Charging Service in Release 8.0.

Group of Ruledefs Configuration Mode

In support for grouped rule categories, a Group of Ruledefs Configuration Mode has been included within the Active Charging Service Mode. This enables grouping rules into categories, so that charging systems can base the charging policy on the category. A group of ruledefs may contain optimizable ruledefs. If all the ruledefs in a group of ruledefs can be optimized, and if the group is included in a rulebase that has optimization turned on, then the group will be optimized.

IP Readdressing

Readdressing of packets based on the destination IP address of the packets is now supported. This enables redirecting unknown gateway traffic to known/trusted gateways.

The IP Readdressing is configured in the flow action defined in a charging action. IP readdressing works for traffic that matches particular ruledef and hence the charging action. IP readdressing is applicable to both uplink and downlink traffic. In the Active Charging Subsystem, uplink packets are modified after packet inspection, rule matching, etc., where the destination IP/port is determined, and replaced with the readdress IP/port just before they are sent out. Downlink packets (containing the readdressed IP/port) are modified as soon as they are received, before the packet inspection, where the source IP/port is replaced with the original server IP/port number.

For one flow from an MS, if one packet is re-addressed, then all the packets in that flow will be re-addressed to the same server. Features like DPI, rule-matching, etc. remain unaffected. Each IP address + port combination will be defined as a ruledef.

In case of IP fragmentation, packets with successful IP reassembly will be readdressed. However, IP fragmentation failure packets will not be re-addressed.

Packet Filter Configuration Mode

In support for the Network Controlled QoS (NCQoS) feature providing control of QoS for subscriber from network element side; i.e. GGSN, a Packet Filter Configuration Mode has been included within the Active Charging Service mode. This mode enables configuring a packet filter’s parameters.

Corrected DCCA Behavior upon Receipt of Charging-Rule-Base-Name AVP

The “Charging-Rule-Base-Name” AVP (code: 1004) is sent in CCA messages from the Gy server to set the rulebase. The rulebase that comes in this AVP must already be configured in the system. In v7.0, ACSMgr checks for the rulebase, and if it is not present discards the message, a CCR-T is not sent. In v7.1 and later, if the rulebase is not present the message is rejected, and a CCR-T is sent with DIAMETER_BAD_ANSWER as the termination cause.

Pipelining of HTTP Requests

ECS now supports pipelining of up to 32 HTTP requests on the same TCP connection. Pipeline overflow requests are not analyzed. Such overflow requests are treated as http-error. The billing system, based on this information, decides to charge or not charge, or refund the subscriber accordingly.

ECS Features in Release 8.1

This section provides information for new features in the Enhanced Charging Service in Release 8.0.

Enhanced Charging Service in Optimized Mode

IMPORTANT

In Release 8.1, Enhanced Charging Service must be enabled in Optimized mode.

In the Optimized mode, ACS Managers (ACSMgrs) are merged with Session Manager (SessMgr), and enhanced charging facilities run as part of the SessMgr. Also, the controller functionality is unified, i.e. the ACS Controller (ACSCtrl) is merged with the Session Controller (SessCtrl).

In the Optimized mode, recovery/reconciliation of ACSCtrl with ACSMgrs is coupled with SessCtrl recovery. I.e., SessCtrl handles recovery of enhanced charging specific configuration. And, reconciliation of ACSCtrl vis-à-vis SRDB tasks is added to SessCtrl reconciliation. SRDB tasks hold the third-party database, which is used for static category-based content-filtering. In Release 8.0, these SRDB tasks are handled by ACSCtrl. In Release 8.1 the SessCtrl controls these SRDB tasks.

The Optimized mode benefits the in-line services that run as part of ECS, i.e. Firewall and Peer-to-Peer with performance improvement.

IMPORTANT

By default, on installing Release 8.1, the system comes up with ECS in non-optimized mode. If the ECS mode is changed from the default (non-optimized) mode to the Optimized mode, or vice-versa, the system must be rebooted for the change to take effect.

IMPORTANT

In UMTS networks, if ECS is configured in the Optimized mode, secondary PDP context traffic does not undergo ECS processing.

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).

Origin-host Encoding for Optimized Mode

The origin host encoding sent in all Diameter messages from the system in the `<instance>-<facility-name>.<origin-host>` format has changed.

In the non-optimized mode, it is encoded as *001-acsmgr.starentnetworks.com.*

In the optimized mode, it is encoded as *001-sessmgr.starentnetworks.com*.

Number of TCP Connections for Optimized Mode

The number of TCP connections established to the Diameter server has changed:

- In the non-optimized mode, it is a maximum of 12 PSC x 6 ACSMgrs.
- In the optimized mode, the number of connections will be <*number of PSC*> x 7 SessMgrs.

ASR in Rel. 7 Gx Implementation Not Supported

In the Rel. 7 Gx implementation, any Abort-Session-Request (ASR) received by the PCEF/BBERF will be treated as an unsupported command. In response, an Abort-Session-Answer (ASA) is sent with DIAMETER_COMMAND_UNSUPPORTED (3001).

Charging Rule Definition Rejection if Precedence AVP Missing in Create Case

In the v8.0 Rel. 7 Gx implementation, when a charging rule definition is sent from PCRF without the Precedence AVP, the default precedence value (255) is populated. Existing precedence of the rule definition changes to the default value (255) even when there is no Precedence AVP in the update.

Now, if the Precedence AVP is missing in the new charging rule definition sent from the PCRF, the default precedence value (255) is not populated, and the charging rule definition is rejected. In the update case, if the Precedence AVP is missing, it is not updated with the default precedence value (255), and the charging rule definition is not rejected. The existing precedence is used.

Pipelining of HTTP Requests

ECS now supports pipelining of up to 32 HTTP requests on the same TCP connection. Pipeline overflow requests are not analyzed. Such overflow requests are treated as http-error. The billing system, based on this information, decides to charge or not charge, or refund the subscriber accordingly.

Default IP for Unsupported Protocol

Unsupported protocol in the flow description is considered as failure and is no longer set with IP as default protocol. In the create case, the rule definition is rejected when this failure happens. In the update case, the existing rule definition is removed when the failure happens.

ESS Features in Release 8.0

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).

Currently, there are no new ESS features in Release 8.0.

ESS Features in Release 8.1

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).

Support for Ignoring Insignificant UDRs

R-ESS introduces new configurables to selectively discard the insignificant UDRS in the database based on a threshold limit in the form of number of total bytes. The statistics of the discarded UDRs will be displayed in Summary Report. Discarding the insignificant UDRs will result in the reduction of the number of records in the database and improvement of the R-ESS reporting performance.

The R-ESS extends its support to include yet another configurable that is set accordingly to enable the collection of parsing statistics report.

Support for Multiple Content Types

This functionality allows the user to select multiple content types from GUI as well as CLI and enables the R-ESS to generate Threshold Content Type and/or Top N Content Type reports based on the selected types. This feature further enables the R-ESS to specify a combined threshold for the selected content types and view the list of users who have used the most amount of traffic for the content types.

Support for Pushing of xDR Files

The L-ESS application extends its support to include some new configurables that are set appropriately to pull the xDR files from ST-series platform and push the files to configured destinations. When this functionality is enabled, L-ESS will start the pull process and file transfer process simultaneously or separately based on the configurations. The L-ESS is configured in such a way that the files are accepted from ST-series platform and then pushed to a central location at L-ESS. The L-ESS pushes the files further to the destinations. The file transfer process will automatically detect the number of hosts and whether they are willing to push EDR / UDR files to L-ESS by detecting the directories present below the configured base path.

Support for Forwarding SNMP Traps to Multiple Destinations

The L-ESS extends its support to include some new parameters in the configuration file, allowing the user to configure up to a maximum of four SNMP destinations for the traps to be forwarded.

Also, a script ‘addhosts.sh’ is modified for addition and removal of Starent and SNMP Manager hosts dynamically. This script is now menu driven and provides option for adding and removing these hosts.

For more information, see the *ESS Installation and Administration Guide*.

Firewall Features in Release 8.0

This section provides information for new features in the Stateful Firewall product in Release 8.0.

ACS and Stateful Firewall Integration

The integration of Stateful Firewall and Enhanced Charging Service in this release has resulted in the following changes:

- Firewall Configuration Mode—This mode is no longer available.
- Firewall ALG Configuration Mode—This mode is no longer available.
- Firewall Policy Configuration Mode—This mode is no longer available.
- ACS Firewall Ruledef Configuration Mode—This new mode is available under the ACS Configuration mode. Firewall rule definitions are configured in this mode.
- Firewall Rulebase Configuration Mode—This mode is no longer available. Both ACS and Firewall ruledefs are now included in ACS rulebases.
- Firewall Host Pool Configuration Mode—Moved under the ACS Configuration Mode, and renamed to ACS Host Pool Configuration Mode.
- Firewall IMSI Pool Configuration Mode—Moved under the ACS Configuration Mode, and renamed to ACS IMSI Pool Configuration Mode.
- Firewall Port Map Configuration Mode—Moved under the ACS Configuration Mode, and renamed to ACS Port Map Configuration Mode.

Firewall Ruledef Configuration Mode

A new Firewall Ruledef Configuration mode is available in Release 8.0 under the ACS Configuration mode. Firewall rule definitions are configured in this mode.

Host Pool, IMSI Pool, and Port Map Support in ACS

The Host Pool, IMSI Pool, and Port Map configuration modes, which were specific to Stateful Firewall configuration, are moved under the ACS Configuration mode for Release 8.0.

Licensing

With this release, if a Stateful Firewall license is installed on the system, Active Charging Services (ACS) will also be enabled. A separate ECSv2 license will not be required to enable ACS. However, if an ECSv2 license is installed on the system, a Firewall license is still required to enable Firewall.

Firewall Features in Release 8.1

This section provides information for new features in the Stateful Firewall product in Release 8.1.

Network Address Translation (NAT)

The NAT feature is used to translate non-routable private IP addresses to routable public IP address(es) from a pool of public IP addresses that have been assigned for NAT. This conserves on the number of public IP addresses required to communicate with external networks, and ensures security as the IP address scheme for the internal network is masked from external hosts, and each outgoing and incoming packet is translated. NAT can be used to perform address translation for simple-IP and mobile-IP.

NAT can be selectively applied to different flows (5 tuple connections) originating from the subscribers based on the flows' L3/L4 characteristics (Source-IP, Source-Port, Destination-IP, Destination-Port, and Protocol). Some flows can be selectively marked for “no NAT” processing based on the flows' L3/L4 characteristics.

NAT works by inspecting both incoming and outgoing IP datagrams and, as needed, modifying the source IP address and port number in the IP header to reflect the configured NAT address mapping for outgoing datagrams. The reverse NAT translations is done for incoming datagrams.

In StarOS 8.1, the NAT feature is only available for UMTS networks.

For more information, see the *Personal Stateful Firewall Administration Guide*.

Policy-based Firewall and NAT Functionality

In StarOS 8.1, Stateful Firewall releases for CDMA networks use rulebase-based configurations. Whereas, while earlier releases of Stateful Firewall and NAT for UMTS networks used rulebase-based configurations, the current releases use policy-based configurations.

In the Policy-based Firewall and NAT implementation, Firewall-and-NAT policies are configured in the ACS Firewall-and-NAT Policy Configuration Mode. Each policy contains a set of ruledefs and the firewall/NAT configurations. Multiple such policies can be configured, however, only one policy is applied to a subscriber at any point of time.

The policy used for a subscriber can be changed either from the CLI, or by dynamic update of policy name in Diameter and RADIUS messages. In both cases NAT status on the active call remains unchanged.

For more information, see the *Personal Stateful Firewall Administration Guide*.

Upgrading to Release 8.1

When upgrading from a pre-8.1 release to 8.1, Firewall must be enabled in the rulebase or the Firewall-and-NAT policy as shown in the following configuration examples.

If the build is 8.1 pre 31st July, use the following configuration:

```
configure
   active-charging service <service_name>
      rulebase <acs_rulebase_name>
         ...
         firewall policy firewall-required
         ...
         exit
```

If the build is 8.1 post 31st July, use the following configuration:

```
configure
   active-charging service <service_name>
      fw-and-nat policy <policy_name>
         ...
         firewall policy firewall-required
         ...
         exit
```

For more information, please contact your local service representative.

GGSN Features in Release 8.0

This section provides information for new features for the GGSN Service in Release 8.0.

Multimedia Broadcast Multicast Service (MBMS)

Starent Networks GGSN now supports Multimedia Broadcast and Multicast Service. The MBMS is an IP datacast type of service in GSM and UMTS cellular network. It eliminates unnecessary replication of data on UMTS wireless networks by transmitting a single stream of data to multiple users. By delivering a single, unidirectional data stream to many subscribers, MBMS makes more efficient use of wireless network resources than traditional point to point connections.

MBMS is a solution for transferring light video and audio clips and also a suitable method for mass communications. MBMS functionality on the system is provided by an existing GGSN and/or SGSN service license. In the absence of a valid license, the system functions as a standard unicast GGSN. When a GGSN is functioning in a MBMS environment, it supports Gmb protocol interface with Broadcast/Multicast Service Center (BM-SC) for messaging.

Figure 1-2 shows the reference architecture of MBMS service in UMTS network.

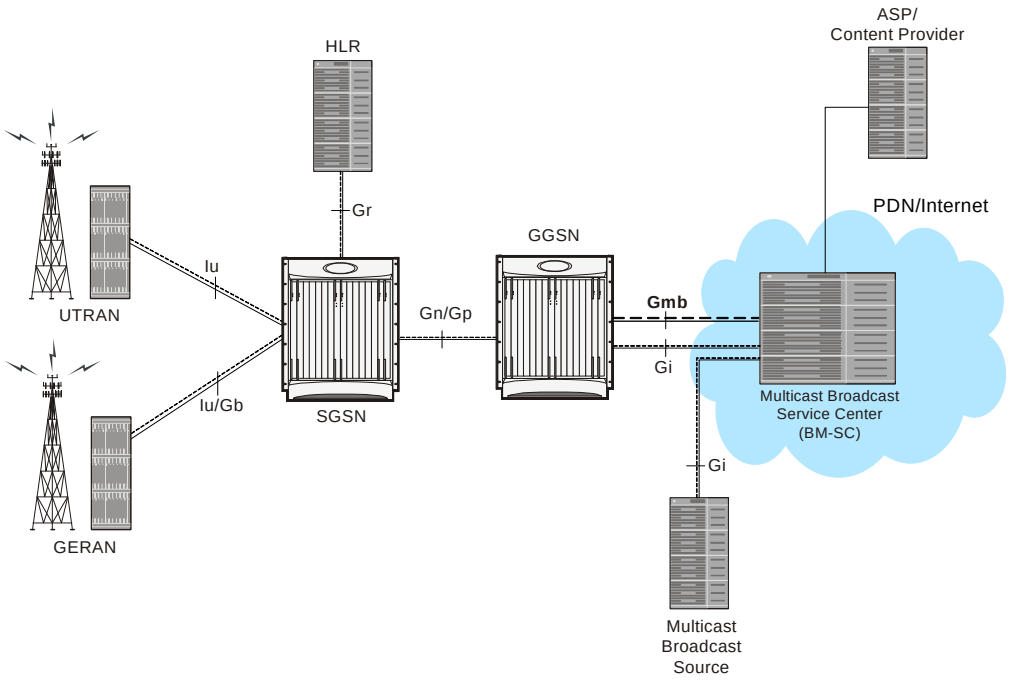


Figure 1-2 MBMS Reference Architecture in UMTS network

For more details on configuration of this service, refer *Multimedia Broadcast and Multicast Service* chapter in *System Enhanced Feature Configuration Guide*.

Network Controlled QoS (NCQoS)

This feature provides control of QoS for subscriber from network element side; i.e. GGSN. It uses bearer control mode and Active Charging Services parameters to provide packet filtering and other quality class identifier related configurations.

Network-controlled QoS is the method by which the QoS for a PDP context (primary or secondary) is updated on the request of the GGSN through Network Requested Update PDP Context (NRUPC) message. It can also activate a new secondary PDP context on Network Requested Secondary PDP Context Activation (NRSPCA) message from the GGSN.

This feature requires separate license key.

For more details on configuration of this service, refer *Dynamic QoS Renegotiation* chapter in *System Enhanced Feature Configuration Guide*.

Traffic Shaping

This is an enhanced feature is a traffic rate limiting method similar to Traffic Policing, however, shaping provides a buffer facility for packets exceeding the configured limit. Once the packets exceed the data-rate, the packets queue inside the buffer to be delivered at a later time.

The bandwidth enforcement can be done in the downlink and the uplink directions independently. If there is no more buffer space available for subscriber data, the system can be configured to either drop the packets or keep them for the next scheduled traffic session.

This feature requires separate license key.

For details on configuring this service, refer to the *Traffic Policing and Shaping* chapter in the *System Enhanced Feature Configuration Guide*.

Direct Tunnel Support

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

The Direct Tunnel architecture allows the establishment of a direct user plane tunnel between the RAN and the GGSN, bypassing the SGSN. The SGSN continues to handle the control plane signalling and typical makes the decision to establish Direct Tunnel at PDP Context Activation. A Direct Tunnel is achieved at PDP context activation by the SGSN establishing a user plane (GTP-U) tunnel directly between RNC and GGSN (using an Update PDP Context Request towards the GGSN).

The following figure illustrates the working of direct Tunnel between RNC and GGSN.

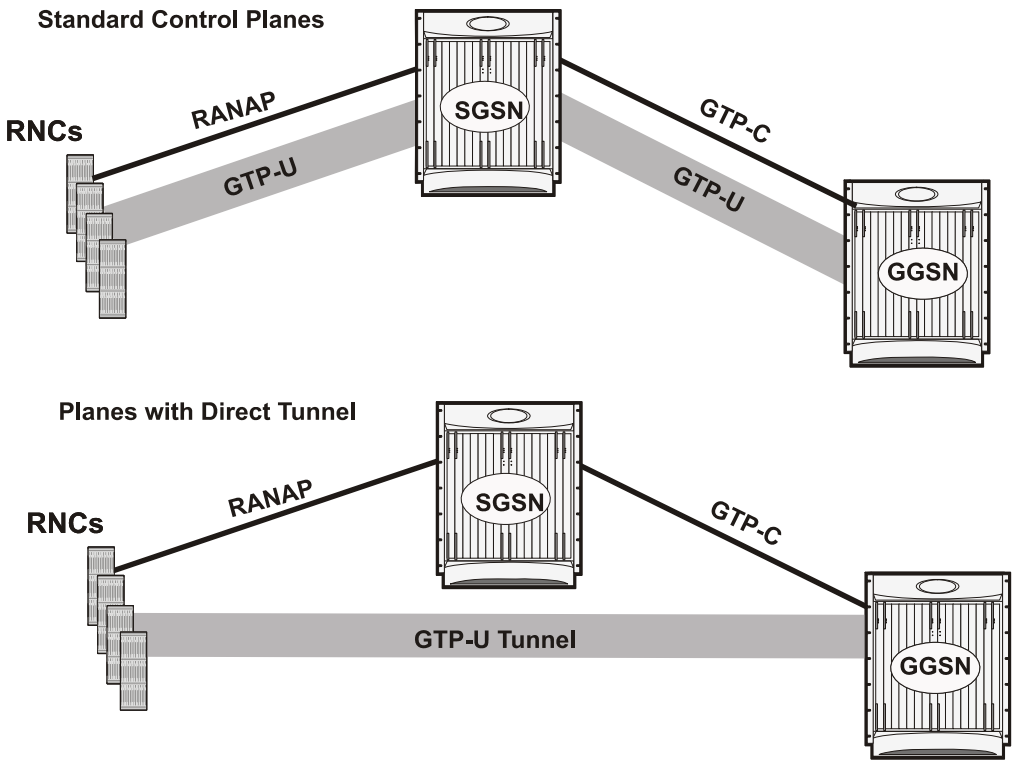


Figure 1-3 Direct Tunnel Support in GGSN

A major consequence of deploying Direct Tunnel is that it produces a significant increase in control plane load on both the SGSN and GGSN components of the packet core. It is therefore of paramount importance to a wireless operator to ensure that the deployed GGSNs are capable of handling the additional control plane loads introduced of part of Direct Tunnel deployment. The Starent GGSN and SGSN offers massive control plane transaction capabilities, ensuring system control plane capacity will not be a capacity limiting factor once Direct Tunnel is deployed.

This feature requires separate license key.

Highest Preference to LNS for DNS Value

DNS query and DNS resolve procedure on system is now modified to support DNS parameters from LNS.

The system will supports configuration of DNS at the Context level in Context configuration with **`ip name-server`** command as well as at the APN level in APN configuration mode with **`dns`** and **`ipv6 dns`** commands, or it can be received from AAA server.

When DNS is requested in PCO configuration, the following preference will be followed for DNS value:

1. DNS Values received from LNS have the first preference.

2. DNS values received from RADIUS Server has the second preference.

3. DNS values locally configured at the APN level has the third preference.

4. DNS values configured at context level has the last preference.

The same preference would be applicable for the NBNS servers to be negotiated via ICPC with the LNS.

CCR (T) Sent after Receiving “Diameter-Credit-Limit-Reached” at Message Level in CCA (I) after Upgrade to v8.0

In the earlier releases, in this scenario, the system did not send a CCR (T) with DIAMETER-ADMINISTRATIVE result-code; the system silently discarded the answer and terminated the session.

In v8.0, the system sends a CCR (T) with DIAMETER_ADMINISTRATIVE as the result-code. System failure-handling can be set to “retry & terminate” (default) or “terminate”.

GGSN Features in Release 8.1

This section provides information for new features for the GGSN Service.

Hard Disk Storage for CDR Files

A hard disk has been introduced in the ST40 platform to add storage capability. When storing CDR files on the SMC hard disk, first they are stored on RAMFS before they are moved to the hard disk and then they can be off-loaded via ftp or sftp to an external server (such as the L-ESS or the GSS) or billing system. For additional support information, see *Hard Disk Support on SMC Card in ST40 Platform*.

- Use the new command **`gtpp storage-server local file {local | remote }`** command in GTPP Group Configuration Mode to configure and enable hard disk usage.
- Use the new show/clear commands **`{ show | clear } gtpp storage-server local file { counter | statistics }`** in the Exec Mode to monitor/clear the file counters and statistics on the hard disk.
- Use the new **`gtpp ram-disk-limit`** and **`gtpp compression-process`** commands in the Global Configuration Mode to allocate RAM for files and the number of compression process to support the hard disk functionality.

NPU Assisted MBMS Data Flow

ST40 platforms now supports NPU assisted processing of MBMS data packets and relieves the Session Manager to provide better performance. Currently with NPU assisted data processing ST40 can support 225 SGSNs per MBMS Bearer Service for downlink of MBMS data. Earlier it was limited to 15.

This enhancement is not applicable to ST16 platforms and a maximum of 15 downlink SGSNs per MBMS Bearer service are supported.

For details about this new enhancement, refer *MBMS Service Configuration* chapter of the *System Enhanced Feature Configuration Guide*.

Rel. 7 Gx Interface Support

Starent Networks GGSN now supports Rel. 7 Gx interface.

For IMS deployment in GPRS/UMTS networks the system uses Rel. 7 Gx interface for policy-based admission control support and flow-based charging. The Rel. 7 Gx interface supports enforcing policy control features like gating, bandwidth limiting, etc., and also supports flow-based charging. This is accomplished via dynamically provisioned Policy Control and Charging (PCC) rules. These PCC rules are used to identify service data flows and do charging. Other parameters associated with the rules are used to enforce policy control.

The PCC architecture allows operators to perform service-based QoS policy, and flow-based charging control. In the PCC architecture, this is accomplished mainly by the Policy and Charging Enforcement Function (PCEF)/Starent Networks GGSN and the Policy and Charging Rules Function (PCRF).

For more information see the *Gx Interface Support* chapter of the *System Enhanced Feature Configuration Guide*.

Quad Gig-E Line Card (QGLC) & Link Aggregation

The GGSN now supports the four-port gigabit-Ethernet line card - QGLC. This card will enable the GGSN to utilize standard-compliant link aggregation. For additional feature information, see *QGLC* and *Link Aggregation* feature descriptions in the *Common Features in Release 8.0* section of this chapter.

For details about this new line card, see the *Hardware Platform Overview* chapter of the *Hardware Installation and Administration Guide*.

GGSN Behavior on QOS Change

The GGSN system now drops uplink/downlink packets when SGSN sends Update PDP Context request for QOS change with maximum bit rate (MBR) as zero for conversational/streaming class of services. This is the default behavior and no configuration required.

Secondary GTPP Group and Enable/Disable CDR Archiving

Regulatory requirements in EU require GGSN to send CDRs to both GSS and CGF while GSS being the billing interface. CDRs sent to CGF should not be buffered and retried in the event the CGF goes down and later comes back. To support this, a secondary GTPP group can be configured under APN, and SessMgr duplicates CDRs to both GTPP groups with a CLI to enable/disable archiving in GTPP group.

Configuring Secondary GTPP Group under the APN

This feature enables configuring a secondary GTPP group in the APN. If the secondary group is configured, when the accounting information is generated, it will also be duplicated to the specified secondary group. This can serve as a backup of the accounting information by sending one record to a GSS server and the other to a CGF server or both to either the GSS/CGF.

Enabling/disabling CDR Archiving in GTPP Group

This enables/disables archiving for CGF only. When enabled, once the server is detected to be down, the request sent to the CGF is purged. Also, the requests generated for the period when the server is down is purged. If a secondary CGF is configured, new requests are directed to the secondary CGF while the requests retried with the primary are purged. By default this is disabled.

Transport Layer Protocol Selection over Ga Interface

Benefits

This new support provides facility to configure the transport layer protocol for Ga interface on AGW (GSNs). Now operator can run Ga interface on TCP as well.

Description

Currently Ga interface between AGW and GTPP server was supported with UDP as default transport layer protocol. To provide connection-oriented session on Ga interface, new configurable feature is to select between UDP and TCP as transport layer protocol for Ga interface. For more information refer **`gtpp transport-layer`** command in *GTPP Server Group Configuration Mode Commands* chapter of *Command Line Interface Reference*.

This feature requires no additional license.

NSAPI Encoding in Diameter

In the earlier releases, the GGSN was encoding ASCII format of the NSAPI in decimal format. NSAPI values of 0 to 9 were encoded in single byte, but values above 10 were encoded as 2 bytes, which lead to faulty message in the OCS.

Now the ASCII format of the NSAPI is encoded in hexadecimal format to restrict the values to one byte.

For example, earlier the value of *10* was encoded as *0x30 0x31* in the byte stream. Now it is encoded as *0x41* in byte stream representing the hexadecimal value *A*.

GSS Features in Release 8.0

This section provides information for new features for the GSS for Release 8.0

Menu-Driven Installation

Also new in this release, a menu-driven installation management interface with quick, simple menu selections for installation, uninstallation, and upgrade processes. For details, refer to the *GTPP Storage Server Installation and Administration Guide*.

SGSN Support

In Release 8.0, GTPP Storage Server (GSS) extends its support to include Serving GPRS Support Nodes (SGSNs), as well as Gateway GPRS Support Nodes (GGSNs), as sources of CDRs to be preserved and managed.

custom4 Format

The custom4 format was created to support writing CDRs in blocks with the FileGen utility. This file format is similar to custom3 file format except CDRs will be written in 2kbyte blocks in a file.

- **Header:** No Header
- **Contents:** CDR1CDR2FFFFFF|CDR3FFFFF..|..CDRnFFFF|
  where | represents the end of a 2k block
- **EoF marker:** No EoF marker
- **File name format**:
  `<GSN_Location>_<date>+<time>_<total-cdrs>_file<fileseqnum>.u`

GSS Features in Release 8.1

This section provides information for new features for the GSS product.

Support for New File Formats

The GTPP Storage Server (GSS) extends its support to include the following file formats:

- Custom5 Format

  This file format is similar to custom3 file format except that the sequence number for CDR file name is of six digits in length ranging from 000001 to 999999.

  - Header: No Header
  - Contents: CDR1CDR2CDR3…CDRn
  - EoF marker: No EoF marker
  - File name format:
    <GSN_Location>_<date>+<time>_<total-cdrs>_file<fixed-length-seqnum>.u
- Custom7 Format

  This customer-specific file format contains CDRs converted from ASN.1 format to ASCII format according to the following conventions. Each line in the file consists of one CDR which contains 33 parameters occupying 491 bytes.

  - Header: No Header
  - Contents: CDR1CDR2CDR3…CDRn
  - EoF marker: No EoF marker
  - File name format:
    Processed_04_YYYYMMDDhhmmss.cdr

IMPORTANT

The custom7 file format is customer-specific. For more information on this file format, contact your local sales representative.

Archive Mode Functionality

In this release, the archive mode functionality is enabled by default during GSS installation without requiring user's input. The default activation is due to the removal of support for non-archive mode.

Support for GTPP Custom Dictionary

In this release, the GTPP Storage Server (GSS) extends its support to include custom12 through custom20 in the GTPP custom dictionaries.

HA Features in Release 8.0

This section provides information for new features in the Home Agent product in Release 8.0.

Mobile IPv6

Benefits

Enables use of single mobility core network for provisioning of IPv6 and IPv4 Mobile IP access services. Mitigates IPv4 address depletion concerns for address intensive always-on applications and interactive applications such as VoIP, video telephony and Push-to-Talk (PTT).

Description

MIPv6 allows a user to maintain a persistent IPv6 address even when handing off between Access Service Networks (ASN's) connected to different ASN GW's and allows the access device to be reachable via the same MIPv6 Home of Address (HoA) irrespective of the current point of attachment. A Mobile IPv6 Node (MN) uses two IPv6 addresses:

- Care of Address (CoA) derived from Interface-ID assigned by DHCP Proxy component on ASN GW after verification of user or device credentials during network access
- Home of Address (HoA) assigned by HA during the Mobile IP registration with home network. The MN registers its current point of attachment by providing its CoA.

The MN can operate in two modes:

- Bidirectional tunnel - In this mode, all data traffic originating from or destined to the MNs MIPv6 HoA is tunneled via the HA.
- Route optimization - In this mode, the MN informs its correspondent node of its current point of attachment, allowing the correspondent node to directly route packets destined to the MN's HoA through its CoA. Route optimization will not be supported in this release.

Supported Features

- MIPv6 message authentication mobility options in binding updates as per RFC 4285
- MN-NAI mobility option in binding messages as per RFC 4283. The MN-NAI option must be included in all Binding messages (Eg initial registration and subsequent updates).
- Native 6-in-6 tunneling between ST40 ASN GW and HA's
- Session-based 6TO4 tunneling between ST40 HA and ST16 ASN GW
- Platform-based 6TO4 tunneling between ST40 HA and adjacent 6BONE gateway routers

Session Continuity Support for 3GPP2 and WiMAX Handoffs

From Release 7.1, this feature provides the seamless session mobility for WiMAX subscriber and other access technology subscribers; i.e. 3GPP2. By implementation of this feature HA can be configured for:

- 3GPP2 HA Service
- 3GPP HA Service
- WiMAX HA Service
- Combination of 3GPP2 and WiMAX HA Service

The above configurations provide the session continuity capability that enables a dual mode device (a multi radio device) to continue its active data session as it changes its active network attachment from 3GPP2 to Wimax and vice versa with no perceived user impacts from a user experience perspective. This capability brings the following benefits:

- common billing and customer care
- accessing home 3GPP2 service through Wimax network and vice versa
- better user experience with seamless session continuity

This feature requires a separate license to enable WiMAX service.

HA Features in Release 8.1

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

Currently, there are no new HA features in Release 8.1.

IP Services Gateway Features in Release 8.0

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

Currently, there are no new IPSG features in Release 8.0.

IP Services Gateway Features in Release 8.1

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

Currently, there are no new IPSG features in Release 8.1.

PDIF Features in Release 8.0

PDIF is not supported in Release 8.0.

PDIF Features in Release 8.1

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

Congestion Control and Overload Disconnect Support

Beginning with the 8.1 release of 01/01/09, PDIF supports congestion control and overload disconnect.

Refer to the “Congestion Control” chapter in the *PDIF Administration Guide,* and to the *Command Line Interface Reference Guide* for more configuration information

Custom DNS Handling

New CLI added to Crypto Template Config Mode: dns-handling { normal | custom }

During IKEv2 session setup, MS may or may not include INTERNAL_IP4_DNS in the Config Payload (CP). PDIF may obtain one or more DNS addresses for the subscriber in DNS NVSE from a proxy-MIP Registration Reply message. If Multiple Authentication is used, these DNS addresses may be also received in Diameter AVPs during the first authentication phase, or in RADIUS attributes in the Access Accept messages during the second authentication phase.

In **`normal`** mode, by default PDIF always returns the DNS address in the config payload in the second authentication phase if one is received from either the configuration or the HA.

`Custom` mode is a new feature added to the CLI for this release to provide an alternative to the default operation. In **`custom`** mode, depending on the number of INTERNAL_IP4_DNS, PDIF supports the variety of behaviors described in the **`custom-dns handling`** section in the “Crypto Template Configuration Mode Commands” chapter of the *CLI Reference Guide*.

DELETE Payload Default Action Change

The IKEv2 stack currently always inserts a DELETE Payload in an INFORMATIONAL DELETE Response from both the PDIF and the MN (WMN).

This default behavior has been updated to not insert a DELETE Payload when the response is from the PDIF.

Note that this behavior is supported by clarifications in RFC 4718.

IPMS Support

IPMS is a licensed feature for PDIF. It provides access to more saved reporting and analysis information. It supports MIBs as they are developed and bulkstats. It must be configured in its own context.

IPMS is described in detail in its own documentation suite, including online help files.

Multiple Authentication

Multiple Authentication is used when setting up a Proxy-Mobile-IP call with PDIF. In Stage One the device is authenticated with an HSS server. In Stage Two, the subscriber is authenticated with a AAA server over a RADIUS interface.

In Stage One, the authentication method must be EAP-AKA. In Stage Two, the authentication must be either MD5 or GTC. If neither MD5 nor GTC is supported, the PDIF can convert these authentication messages and use standard PAP/CHAP authentication instead.

This is fully described in the “PDIF Overview” chapter in the *PDIF Administration Guide.*

Online Upgrade

PDIF is now using an online upgrade model called Active-Standby. This requires a license to activate. Two chassis are connected by a redundancy link and Service Redundancy Protocol (SRP) is used over the link to monitor and control chassis state. Both active and standby chassis have SRP-Activated resources defined. Loopback interfaces are used in the example in the Admin Guide.

"SRP-Activated" means that the resource is configured with **`srp-activate`** to make the protocol work between the two chassis. These resources are the same between the Active and Standby PDIF. Loop-back IP addresses in Ingress and Egress contexts and IP pools in egress contexts are usually SRP-Activated resources. Only the active chassis enables the SRP-Activated resources.

Online upgrade is discussed in the *PDIF Administration Guide*.

SRP and other required commands are documented in the *Command Line Interface Reference*.

Public and Private Key Mismatch Check

PDIF supports x.509 certificates. Every certificate has a public key of its own and configuration on a PDIF is done with the public key and a private key. A mechanism has now been added to verify the AUTH payload from PDIF using PDIF’s public key. If there is a mis-match in the keys, you now see the following warning:

```
Failure: Public and Private key given for certificate does not match!
```

Session Recovery

Session Recovery is now a licensed feature for PDIF. It is described in the “PDIF Session Recovery” chapter of the *Enhanced Features Guide* and is also described in the PDIF Admin Guide.

It is activated by the CLI **`require session recovery`** in the Global Config mode.

PDIF Features in Release 8.3

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

Multiple IPSec Traffic Selectors

Beginning with Release 8.3, the PDIF supports multiple IPsec 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.

For more information, see the chapters “Packet Data Interworking Function Overview” and “Configuration” in the *PDIF Administration Guide*.

Selective Diameter Profile Update Request Control

Beginning with Release 8.3, the PDIF includes a selective Diameter Profile Update Request Control feature. For mobile IP calls, this feature allows WiFi data-only sessions to co-exist with VoIP sessions on the PDIF platform.

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.

This feature is enabled by default and requires no configuration.

For more information, see the chapter “Packet Data Interworking Function Overview” in the *PDIF Administration Guide*.

PDSN Features in Release 8.0

This section provides information for new features in the Packet Data Serving Node in Release 8.0.

Traffic Shaping

This is an enhanced feature for the 8.0 release and is a traffic rate limiting method similar to the Traffic Policing, but it provides a buffer facility for packets exceeded the configured limit. Once the packet exceeds the data-rate, the packet queued inside the buffer to be delivered at a later time. Requires separate license key.

The bandwidth enforcement can be done in the downlink and the uplink direction independently. If there is no more buffer space available for subscriber data system can be configured to either drop the packets or kept for the next scheduled traffic session.

For more details on configuration of this service, refer *Traffic Policing and Shaping* chapter in *System Enhanced Feature Configuration Guide*.

PDSN Features in Release 8.1

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

Currently, there are no new PDSN features in Release 8.1.

Peer-to-Peer Features in Release 8.0

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

Currently, there are no new P2P features in Release 8.0.

Peer-to-Peer Features in Release 8.1

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

IMPORTANT

The P2P features in this section are all available in Release 8.1 only.

P2P Protocols supported for detection

With release 8.1, the system supports detection of the following P2P protocols:

- aol

IMPORTANT

The AOL protocol is detected as Oscar.

- applejuice
- ares
- ddlink
- directconnect
- feidian
- filetopia
- fring
- gadu_gadu
- halflife2
- hamachivpn
- imesh
- irc
- iskoot
- manolito
- mute
- oscar
- pando
- popo
- pplive
- ppstream
- qq
- qqlive
- skinny
- sopcast

- soulseek
- steam
- tvants
- tvuplayer
- uusee
- vpnx
- vtun
- winmx
- wofwarcraft
- xbox
- zattoo

SGSN Features in Release 8.0

This section provides information for new features (listed alphabetically) in Release 8.0 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*.

Limits / Engineering Rules

The following limits for releases 8.0, 8.1, and 9.0 have been modified in the Engineer Rules appendix of the *SGSN Administration Guide*.

- 2G Gb over FR Intf: Max NSEs controlling the same RA increased from 16 to 64
- 2G Gb over IP Intf: Max NSEs controlling the same RA increased from 16 to 64
- 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.

1-in-N IMEI Checks for Subscriber Events

The IMEI check procedure is performed to avoid fraudulent usage of mobile equipment. At attach, when a subscriber registers with an SGSN, the SGSN retrieves the MS equipment identity and then sends a “Check_IMEI” request to the EIR.

The EIR maintains a database of all equipment. The database is organized in three lists – white, gray, and black lists. The EIR checks the three lists to determine on which list the MS’ equipment identity belongs. Then the EIR returns the status request back to the SGSN with the list information.

- If the equipment status is black-listed, the SGSN does not allow the mobile to register with the SGSN.
- If the equipment status is white-listed, the SGSN proceeds with the registration.
- If the equipment status is gray-listed, the default handling is to allow the registration, which can be overridden via the SGSN CLI.

The number of IMEI checks is configured with the **`check-imei-every-n-events`** keyword of the **`equipment-identity-register`** command in the MAP Service configuration mode. The feature is enabled with the **`verify-equipment-identity`** keyword of the **`gmm retrieve-equipment-identity imei`** command in the SGSN Operator Policy

configuration mode. See the appropriate configuration mode chapters in the *CLI Reference Guide* for details.

1-in-N Selective Authentication of Subscriber Events

The SGSN Operator Policy now provides a mechanism to configure selective re-authentication and / or P-TMSI re-allocation for 3G events, where an event is one of the following: an attach request, a RAU, a service request, an activate primary PDP context request, a detach request. The N frequency range is 1 to 16. Configuration means that N minus 1 events are skipped before authentication occurs. For configuration details, see the **`authenticate`** command in the *SGSN Operator Policy Configuration Mode* chapter of the *CLI Reference Guide*.

2.5G/3G Dual Access

Within the same chassis, the SGSN can simultaneously operate as both a 2.5G SGSN and a 3G SGSN. This co-location has been done without proprietary protocols thus avoiding problems with mobility and handoff. Dual access provides a range of benefits, such as: use of the same hardware, load sharing, and the need for fewer IP addresses.

Attach Rate Throttle

It is unlikely that the SGSN would become a bottleneck because of the SGSN's high signaling rates. However, other nodes in the network may not scale commensurately. To provide network overload protection, the SGSN provides a mechanism to control the number of attaches occurring through it on a per second basis.

Fractional E1/DS1 Support

The SGSN, using the Channelized Line Cards, now supports fractional E1/DS1 with up to 8 configurable groupings of timeslots per port. This feature is configured with a combination of the **`path`** and **`frame-relay`** commands in the *Channelized Port Configuration Mode* chapters of the CLI Reference Guide.

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 Radio-Network-Controller 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.

Ga Interface to the CGF/GSS

The SGSN now supports the Ga interface to the CGF for accounting purposes. The SGSN uses the Ga interface to communicate with the charging gateway function (CGF) or the GTPP Storage Server (GSS) using GTP Prime (GTPP). The charging gateway is responsible for buffering and pre-processing billing records. One or more Ga interfaces can be configured per system context. This interface is supported through the following commands in the Context configuration Mode:

- gtpp charging-agent address
- gtpp duplicate-hold-time minutes
- gtpp echo-interval
- gtpp max-cdrs
- gtpp max-pdu-size
- gtpp max-retries
- gtpp redirection-allowed
- gtpp server
- gtpp storage-server
- gtpp timeout

Gb-Flex - SGSN Pooling

The SGSN, with its high capacity, signaling performance, and peering capabilities combined with its level of fault tolerance, delivers many of the benefits of ***Flex*** functionary even without deploying SGSN pooling.

As defined by 3GPP TS 23.236, the SGSN implements Gb-Flex functionality to ensure SGSN pooling for 2.5G accesses as both separate pools and as dual-access pools. SGSN pooling enables the following:

- Eliminates the single point of failure between a BSS and an SGSN.
- Ensures geographical redundancy, as a pool can be distributed across sites.
- Minimizes subscriber impact during service, maintenance, or node additions or replacements.
- Increases overall capacity via load sharing across the SGSNs in a pool.
- Reduces the need/frequency for inter-SGSN RAUs. This substantially reduces signaling load and data transfer delays.
- Supports load redistribution with the SGSN off loading procedure.

Gs Interface to the MSC/VLR

In Release 8.0, the SGSN now supports the Gs interface to the MSC/VLR. This interface is vital in the call-setup process as these databases provide authentication information about MS/UEs attempting to attach.

The Gs Service Configuration Mode has been added to configure and manage the Gs interface between the SGSN and the MSC/VLR. This new mode includes the following commands:

- associate-sccp-network
- bssap+
- default
- end
- exit
- max-retransmission
- non-pool-area
- pool-area
- timeout
- vlr

The new commands will be found the chapter titled *Gs Service Configuration Mode Commands* in the ***Command Line Interface Reference***.

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.

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.

Network-Initiated PDP Context Activation

SGSN now supports standards compliant network-initiated PDP context activation. The network, or actually the GGSN, is not actually initiating the PDP context activation - it is requesting the MS/UE to activate the PDP context.

QoS Traffic Policing per Subscriber

The SGSN now offers QoS traffic policing which enables the operator to configure and enforce bandwidth limitations on individual PDP contexts of a particular traffic class. Traffic policing typically deals with eliminating bursts of traffic and managing a traffic flow in order to comply with a traffic contract.

The SGSN conforms to the DiffServ model for QoS by handling the 3GPP defined classes of traffic, QoS negotiation, DSCP marking, traffic policing, and support for HSDPA/HSUPA.

The SGSN can police uplink and downlink traffic according to predefined QoS negotiated limits fixed on the basis of individual contexts - either primary or secondary. The SGSN employs the Two Rate Three Color Marker (RFC2698) algorithm for traffic policing.

For more information, see the *SGSN Overview* in the *Product Overview* and the *Traffic Policing and Shaping* and *Dynamic QoS Renegotiation* chapter in *System Enhanced Feature Configuration Guide*.

Session Recovery Support

The session recovery feature, now available for both 2G and 3G SGSNs, handles SGSN services for all attached and/or activated subscribers. When enabled, session recovery provides seamless failover and reconstruction of subscriber session information in the event of a hardware or software fault within the system preventing a fully connected user session from being disconnected.

This is an enhanced feature and requires a separate license key to be enabled with the SGSN service. For more information on session recovery, refer to the *System Enhanced Feature Configuration Guide*.

Short Message Service - SMS

The SGSN implements a configurable short message service (SMS) to send and receive text messages up to 140 octets in length. The SGSN handles multiple, simultaneous messages of both types: those sent from the MS/UE (SMS-MO: mobile originating) and those sent to the MS/UE (SMS-MT: mobile terminating).

After verifying a subscription for the PLMN’s SMS service, the SGSN connects with the SMSC (short message service center), via a Gd interface, to relay received messages (from a mobile) using MAP-MO-FORWARD-REQUESTs for store-and-forward. In the reverse, the SGSN awaits messages from the SMSC via MAP-MT-FORWARD-REQUESTs and checks the subscriber state before relaying them to the target MS/UE. The SGSN will

employ both the Page procedure and MNRG (mobile not reachable for GPRS) flags in an attempt to deliver messages to subscribers that are absent.

The SGSN supports both charging for SMS messages (MO - mobile originating and MT - mobile terminating) and lawful intercept of SMS-MO and SMS-MT messages.

Configuration for the service is explained in the ***SGSN Administration Guide***. The various CLI used to enable and configure the SMS service are defined in the Command Line Interface Reference.

CLI

- SMS is enabled with the **`short-message-service`** command in the MAP Service configuration mode. Entering this command accesses the SMS Service configuration mode with the commands to define the SMS service operational configuration:

```
[cntxt_name]st40(config-map-service-serv_name)# short-message-service
[cntxt_name]st40(config-map-service-serv_name-sms-service)#
```

HSPA Fallback (aka Data Rate Management per RNC)

Benefits

Configurable control of data rates on a per RNC basis enables operators to allow subscribers to roam in and out of coverages areas with different QoS levels.

Description

The SGSN can now limit data rates (via QoS) on a per-RNC basis. Some RNCs support HSPA rates (up to 16 Mbps in the downlink and 8 Mbps in the uplink) and cannot support higher data rates - such as those enabled by HSPA+ (theoretically, up to 256 Mbps both downlink and uplink). Being able to specify the QoS individually for each RNC makes it possible for operators to allow their subscribers to move in-and-out of coverage areas with different QoS levels, such as those based on 3GPP Release 6 (HSPA) and 3GPP Release 7 (HSPA+).

For example, when a PDP established on an RNC with 21 Mbps is handed off to an RNC supporting only 16 Mbps, the end-to-end QoS will be re-negotiated to 16 Mbps. Note that an MS/UE may choose to drop the PDP during the QoS renegotiation to a lower value.

This data rate management per RNC functionality is enabled, in the RNC configuration mode, by specifying the type of 3GPP release specific compliance, either release 7 for HSPA+ rate or pre-release 7 for HSPA rates. For configuration details, refer to the *RNC Configuration Mode* chapter in the *Command Line Interface Reference* (version 8.x).

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
.
.
```

SGSN Behavior - Modified for Release 8.0

NSE related limits, which are not configurable, have been modified for release 8.0 only:

- Number of NSEs was 1024, now is 256
- Number of local NSVLs was 4, now is 4
- Number of peer NSVLs per NSE was 16, now is 64
- Number of NSVCs per IP-NSE was 64, now is 256
- Number of NSVCs per FR-NSE was 64, now is 128

SGSN Features in Release 8.1

This section provides information for new features in the Serving GPRS Support Node (SGSN) product.

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.

Direct Tunnel Support

In accordance with standards, one tunnel functionality enables the SGSN to establish a direct tunnel at the user plane level - a GTP-U tunnel, directly between the RAN and the GGSN.

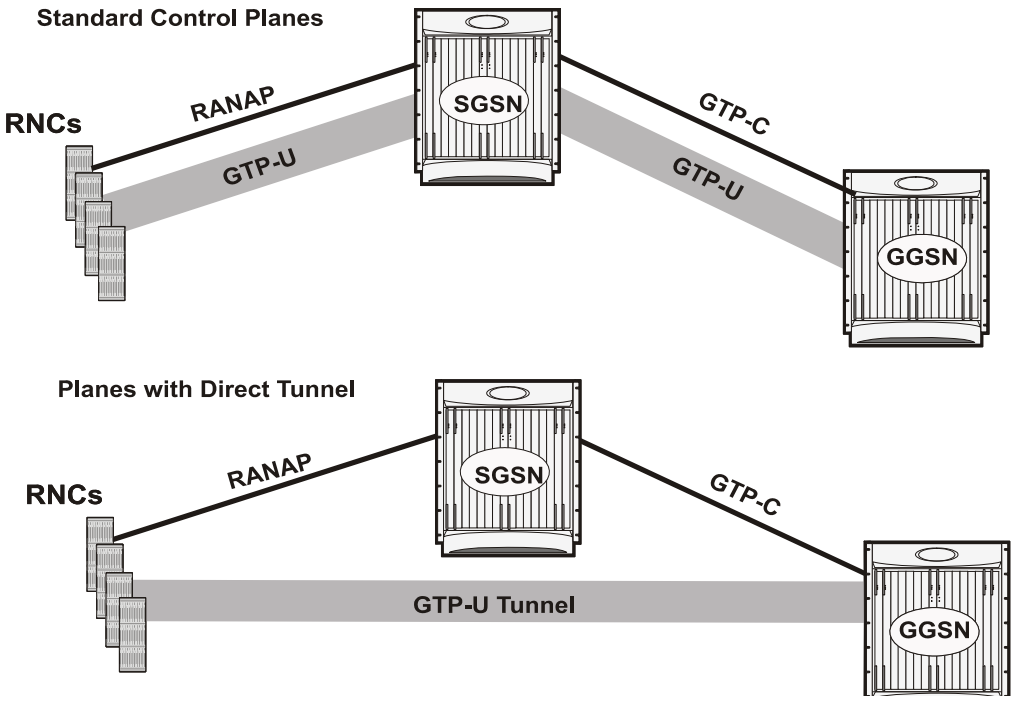


Figure 1-4 SGSN Direct Tunnel

The SGSN typically establishes a direct tunnel at PDP context activation using an update PDP context request towards the GGSN.

In effect, a direct tunnel reduces data plane latency as the tunnel functionality acts to remove the SGSN from the data plane and limit the SGSN to the control plane for processing. This improves the user experience (e.g., expedites web page delivery, reduces round trip delay for conversational services). Additionally, direct tunnel functionality implements the standard “SGSN optimization” to improve the usage of user plane resources (and hardware) by removing the requirement from the SGSN to handle the user plane processing.

Direct tunnel means a significant increase in control plane load on both the SGSN and GGSN components of the packet core. Hence, deployment requires highly scalable GGSNs since the volume and frequency of *update PDP context* messages to the GGSN will increase substantially. Platform capabilities ensure control plane capacity will not be a limiting factor with direct tunnel deployment.

For more information on Direct Tunnel configuration, refer to *SGSN Direct Tunnel Configuration* chapter in *System Enhanced Feature Configuration Guide*.

This features requires a special license.

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.

Ga Interface Supports Configurable Transport Layer

It is now possible to configure the transport layer from the standard UPD to TCP. This functionality has been added to enable the carrier to select connection-oriented sessions for the Ga interface. For more information, refer to the **`gtpp transport-layer`** command in the *GTPP Group Configuration Mode* chapter of the *Command Line Interface Reference*.

Hard Disk Storage for CDR Files

A hard disk has been introduced in the ST40 platform to add storage capability. When storing CDR files on the SMC hard disk, first they are stored on RAMFS before they are moved to the hard disk and then they can be off-loaded via ftp or sftp to an external server (such as the L-ESS or the GSS) or billing system. For additional support information, see *Hard Disk Support on SMC Card in ST40 Platform*.

- Use the new command **`gtpp storage-server local file {local | remote }`** command in GTPP Group Configuration Mode to configure and enable hard disk usage.
- Use the new show/clear commands **`{ show | clear } gtpp storage-server local file { counter | statistics }`** in the Exec Mode to monitor/clear the file counters and statistics on the hard disk.
- Use the new **`gtpp ram-disk-limit`** and **`gtpp compression-process`** commands in the Global Configuration Mode to allocate RAM for files and the number of compression process to support the hard disk functionality.

IuFlex / SGSN Pooling

The SGSN supports 2G Gb Flex with SGSN Pooling and now 3G Iu Flex with SGSN Pooling as an orderable feature.

Iu Flex and SGSN Pooling functionality has been implemented according to 3GPP TS23.236. The SGSN supports pooling for both 3G and 2G accesses, both as separate pools and as dual-access pools.

IuFlex works by defining NRIs in the SGSN service and configuring RNCs as pooled. Pooled RNCs will be able to co-exist with RNCs that are connected to only one SGSN.

Iu Flex offloading is also enabled via configuration. This implementation allows carriers to load balance sessions among pooled SGSNs; where Iu Flex provides carriers deterministic failure recovery.

Additional benefits of Iu Flex include:

- Enables geographical redundancy, as a pool can be distributed across sites.
- Increases overall capacity, as load sharing across the SGSNs in a pool is possible.
- Reduces signaling load as well as data transfer due to conversion of inter-SGSN RAUs to intra-SGSN RAUs for moves between RAs controlled by the same pool.
- Simplifies introduction of new nodes and replacement of old nodes as subscribers can be moved in a planned manner to new nodes.
- Eliminates single point of failure between an RNC/BSS and SGSN.
- Enables service downtime for maintenance scheduling.

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.

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 (2.5G only)

With this new feature, the 2.5G SGSN supports cell-sites with more than one PLMN-ID. Operators can now assign a different PLMN-ID to each cell in the network (typically, there are no more than 3 or 4 PLMN-IDs in a single network). This multiple PLMN support also enables an operator to 'hire out' their infrastructure to other operators who wish to use their own PLMN-IDs. Each cell can be part of only one PLMN (one GRPS service). By configuring the GPRS service for each PLMN-ID, this feature allows the 2.5G SGSN to perform handovers between the service instances.

Configuring Multiple PLMN Support:

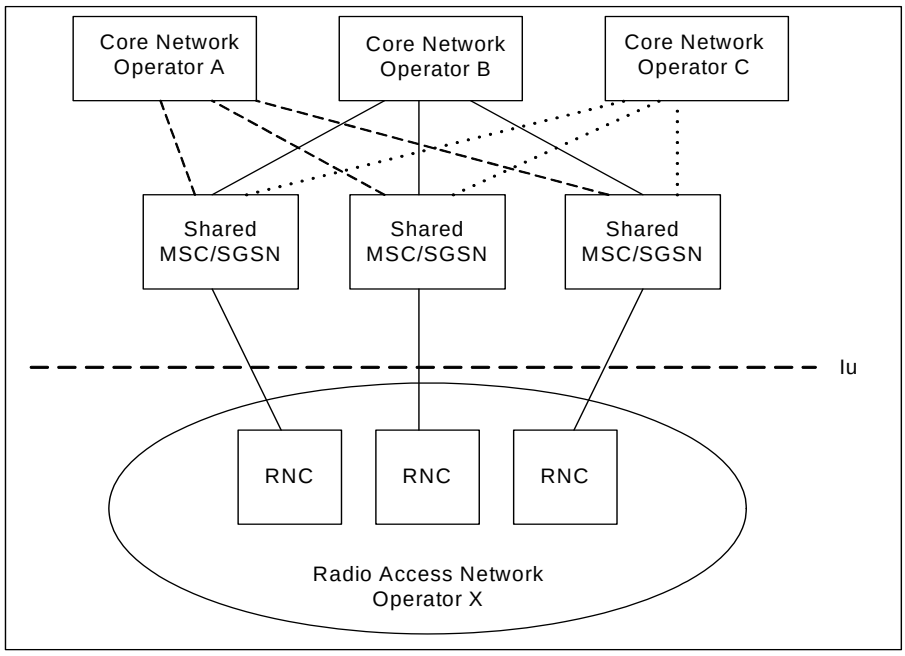
The 2.5G SGSN supports MS handover from one PLMN to another PLMN by configuring multiple instances of the GPRS service, each with a different PLMN-ID, in the same context. Each of the GPRS services must use the same MAP, SGTPU and GS services so these only need to be defined one-time per context. For command details, refer to the *GPRS Service Configuration Mode* and *MAP, SGTP, and GS Service Configuration Mode* chapters in the *Command Line Interface Reference.*

To enable appropriate S-CDR generation in a multiple PLMN-ID scenario, use the **`plmn-id-change`** keyword for the **`gtpp trigger`** command in the GTPP Group Configuration Mode also documented in the *CLI Reference*.

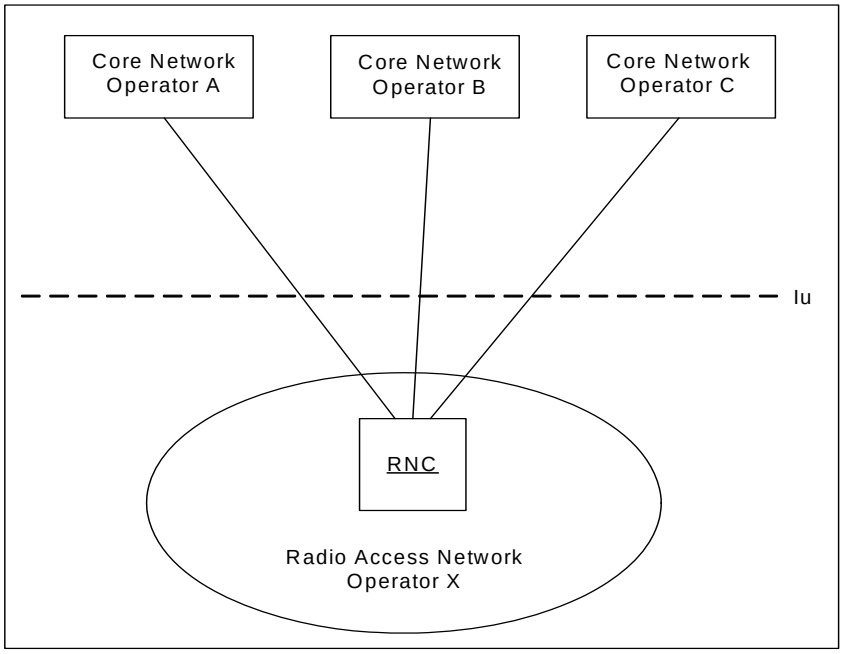
Network Sharing

The SGSN enables two or more network operators to share common network infrastructure. In accordance with 3GPP TS 23.251, the SGSN supports two different configurations for network sharing based on the resources being shared: gateway core network (GWCN) and multi-operator core network (MOCN).

With GWCN, the complete radio access network and partial core network are shared among different operators. Each operator will have its own network node for GGSN/HLR, etc., while sharing SGSN/MSC and the remaining radio network.



With MOCN, the complete radio network is shared among different operators, while each operator maintains its own separate core network.



With these two configurations, the SGSN supports multiple scenarios such as MOCN with non-supporting UE, MOCN with supporting UE, GWCN with supporting UE, and GWCN with non-supporting UE.

NPU FastPath

The NPU FastPath feature is proprietary and only available on the ST40 SGSN systems. The purpose of this type of internal direct tunnel is to optimize resource usage and reduce latency when processing GTP-U packets. Incoming traffic passes through the switch fabric and the routing headers are changed to re-route traffic from the incoming network processing unit (NPU) of the ingress PSC directly to the outgoing NPU of the egress PSC. This means that intervening NPUs and CPUs are by-passed. This provides the SGSN with router-like latency and increased node signaling capacity.

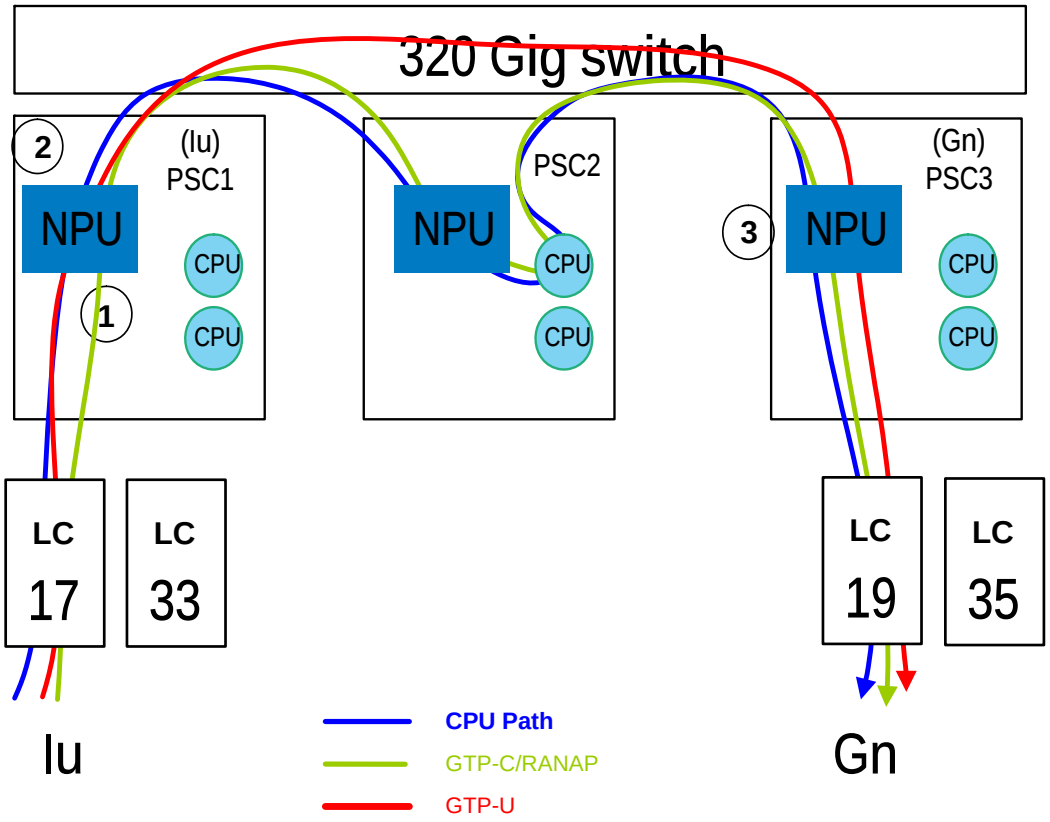


Figure 1-5 SGSN NPU FastPath

Fast path is established when both ends of a tunnel are available. Two fast path flows are established, one for the uplink and one for the downlink direction for a given PDP context.

If FastPath cannot be established, the NPU forwards the GTP-U packets to a CPU for processing and they are processed like all other packets.

FastPath can not be established for subscriber PDP sessions if:

- Traffic Policing is enabled
- Subscriber Monitoring is enabled
- Lawful Intercept (LI) is enabled
- IP Source Violation Checks are enabled
- GTP-v0 tunnel is esatlished with a GGSN

FastPath will be dropped temporarily during:

- Intra-SGSN RAU
- Iu-connection release

Quad Gig-E Line Card (QGLC) & Link Aggregation

The SGSN now supports the four-port gigabit-Ethernet line card - QGLC. This card will enable the SGSN to utilize standard-compliant link aggregation. For additional feature information, see *QGLC* and *Link Aggregation* feature descriptions in the *Common Features in Release 8.0* section of this chapter.

For details about this new line card, see the *Hardware Platform Overview* chapter of the *Hardware Installation and Administration Guide*.

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
.
.
```

Traffic Handling - QoS Provisioning with ARP

The SGSN now enables setting the priority of service via the configuration of the allocation/retention priority (ARP) IE. By including this IE in the RANAP message during the RAB assignment procedure it is possible to specify the relative importance of the radio access bearers for the allocation and retention of traffic. When there is a resource crunch, the IE is used by the RNC to allocate or deallocate resources according to the defined priority. This IE also tells whether queuing of packets is allowed or not.

Although the HLR subscription record only provides a single priority parameter (values 0 to 3), the RNC needs additional information, which our configuration command maps to the subscription priority. Additional information needed:

- Priority Level: 1..15
- Pre-emption Capability: shall-not-trigger-pre-emption, may-trigger-pre-emption
- Pre-emption Vulnerability: pre-emptable, not-pre-emptable
- Queuing Allowed: queuing-not-allowed, queuing-allowed

For configuration details, see *SGSN APN Configuration Mode* in the *CLI Reference Guide*.

CLC2 - Channelized Line Card 2

For Frame Relay signaling, the SGSN now supports the Channelized Line Card 2 (CLC2), the next-generation SONET/SDH channelized line card for the ST40. In North America, the card supplies ANSI SONET STS-3 (optical OC-3) signaling. In Europe, the card supplies SDH STM-1 (optical OC-3). The transmission rate for the card is 155.52 Mb/s with 336 SONET channels supplying T1 and 252 SDH channels supplying E1. The CLC2 is RoHs 6/6 compliant. Each CLC2 provides four optical fiber physical interfaces (ports). For more information about this card, refer to the ***ST40 Hardware Installation and Administration Guide***.

OLC2 - Optical Line Card 2

For ATM signaling, the SGSN now supports the Optical Line Card 2 (CLC2), the next-generation SONET/SDH optical line card for ATM signaling on the ST40. The OLC2 supports all features, including 4 ports, available on the original OLC but now includes RoHs 6/6 compliance. For more information about this card, refer to the ***ST40 Hardware Installation and Administration Guide***.

Web Element Manager Features in Release 8.0

This section provides information for new features for the Web Element Manager application in Release 8.0.

Support for Configurable DSCP Marking Based on Allocation/Retention Priority

GGSN now supports configurable DSCP marking based on traffic handling priority and allocation/retention priority for the Interactive Traffic class. A DSCP value matrix is introduced and used to map based on these priorities only if the allocation priority is present in the QOS profile.

Web Element Manager Path

Click **Configuration | GGSN | GGSN Service | Add / Modify GGSN Service Configuration Dialog Box - Timers/QoS** tab.

Click **Configuration | GGSN | GGSN Service | GGSN Service Details Configuration Dialog Box**.

Click **Configuration | GGSN | APN | APN Configuration Dialog Box - Tunnel / Qos** tab.

Click **Configuration | GGSN | APN | Add / Modify APN Configuration Dialog Box - Tunnel / Qos** tab.

Support for SGSN Bulk Statistics

WEM now provides support for SGSN bulk statistics. Multiple bulk statistic counters are introduced and grouped according to the following SGSN schemas:

- SGSN Schema: These are variables per SGSN service and uniquely identified by SGSN service name and VPN context.
- SCCP Schema: Each SCCP network is uniquely identified by a number in the chassis. All the statistics in this schema are per sccp-network.
- SGTP Schema: These are variables per SGTP service and identified uniquely by SGTP service name and VPN context.
- SS7RD Schema: Each SS7-routing domain is identified by a number unique across the chassis. All the statistics in this schema are per ss7rd.

Support for SGSN Alarms/Traps in Web Element Manager

WEM now supports a new set of traps related to the SGSN services and sessions:

- starSGSNServiceStart
- starSGSNServiceStop
- starM3UAPCUnavailable
- starM3UAPCAvailable
- starM3UAASDown
- starM3UAASActive
- starM3UAASPDown
- starM3UAASPUp
- starSCCPSspRcvd
- starSCCPSspClear
- starSGSNRNCReset
- starSGSNHLRReset
- starSGSNGtpcPathFailure
- starSGSNGtpcPathFailureClear
- starSGSNGtpuPathFailure
- starSGSNGtpuPathFailureClear
- starMTP3LinkOutOfService
- starMTP3LinkInService
- starMTP3LinkSetUnavailable
- starMTP3LinkSetAvailable
- starSCTPAssociationFail
- starSCTPAssociationEstablished
- starSCTPPathDown
- starSCTPPathUp
- starThreshSGSNSessions
- starThreshClearSGSNSessions
- starThreshPerServiceSGSNSessions
- starThreshClearPerServiceSGSNSessions
- starThreshSGSNPdpSessions
- starThreshClearSGSNPdpSessions
- starThreshPerServiceSGSNPdpSessions
- starThreshClearPerServiceSGSNPdpSessions

Support for Content Filtering Report Configuration

WEM provides support for ad hoc generation of reports.

Web Element Manager Path

Click **Accounting | Content Filtering | Report Configuration**.

Click **Accounting | Content Filtering | View Reports**.

Web Element Manager Features in Release 8.1

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

Support for PDIF functionality

This functionality provides the various configurables to configure PDIF and obtain the PDIF bulkstats.

Web Element Manager Path

Click **Configuration | PDIF | PDIF Service | PDIF Service Dialog Box – General / AAA/HSS** tab.

Click **Configuration | PDIF | PDIF Service | Add/Modify PDIF Service Dialog Box – General / AAA/HSS** tab.

Click **Performance | PDIF | PDIF Statistics Dialog Box**.

Support for IKEv2 Transform Set

WEM provides PDIF support for the IKEv2 IKE Security Association and IP Security transform sets.

Web Element Manager Path

Click **Configuration | Context Provisioning | IP Security | IKEv2 IKESA Transform Set | IKEv2 IKESA Transform Set Configuration Dialog Box**.

Click **Configuration | Context Provisioning | IP Security | IKEv2 IKESA Transform Set | Add/Modify IKEv2 IKESA Transform Set Dialog Box**.

Click **Configuration | Context Provisioning | IP Security | IKEv2 IPSEC Transform Set | IKEv2 IPSEC Transform Set Configuration Dialog Box**.

Click **Configuration | Context Provisioning | IP Security | IKEv2 IPSEC Transform Set | Add/Modify IKEv2 IPSEC Transform Set Dialog Box**.

Support for Crypto Template

WEM provides PDIF support for the crypto template. The Crypto Template Configuration Mode is used to configure an IKEv2 PDIF IPSec policy. A PDIF service will not function without a configured crypto template. Only one crypto template can be configured per PDIF service.

The Crypto Template Payload Configuration Mode is used to assign the correct IPSec transform set from a list of up to four different transform sets, and to assign Mobile IP addresses.

Web Element Manager Path

Click **Configuration | Context Provisioning | IP Security | Crypto Template | Crypto Template Configuration Dialog Box - General / IKEv2 IKESA/Authentication / Payload** tab.

Click **Configuration | Context Provisioning | IP Security | Add/Modify Crypto Template | Crypto Template Configuration Dialog Box - General / IKEv2 IKESA/Authentication / Payload** tab.

Support for IPv6

WEM provides PDIF support for IPv6 Neighbors, IPv6 Route, and IPv6 Interface Summary.

Web Element Manager Path

Click **Configuration | Context Provisioning | IPv6 Neighbors | IPv6 Neighbor Configuration Dialog Box**.

Click **Configuration | Context Provisioning | IPv6 Neighbors | Add IPv6 Neighbor Dialog Box**.

Click **Configuration | Context Provisioning | IPv6 Route | IPv6 Route Configuration Dialog Box**.

Click **Configuration | Context Provisioning | IPv6 Route | Add/Modify IPv6 Route Dialog Box**.

Click **Performance | IPv6 Interface Summary | IPv6 Interface Summary Dialog Box**.

Support for Diameter Configuration

WEM provides PDIF support to configure the Diameter Endpoint and Diameter Authentication configuration.

Web Element Manager Path

Click **Configuration | Context Provisioning | Diameter Configuration | Diameter Endpoint**.

Click **Configuration | Context Provisioning | Diameter Configuration | Diameter Authentication**.

Support for URL Blacklisting Statistics

WEM provides support for the URL Blacklisting Statistics.

Web Element Manager Path

Click **Performance | Active Charging | URL Blacklisting Statistics**.

Support for Content Filtering Statistics

WEM provides support for the Content Filtering and Category Database Statistics.

Web Element Manager Path

Click **Performance | Active Charging | Content Filtering Statistics**.

Click **Performance | Content Filtering | Content Filtering Statistics**.

Click **Performance | Content Filtering | Category Database Statistics**.

Support for EAP Profile

WEM provides support for the EAP Profile functionality.

Web Element Manager Path

Click **Configuration | Context Provisioning | EAP Profile**.

Support for Certificate Configuration

WEM provides support for Certificate configuration and Private Key configuration.

Web Element Manager Path

Click **Configuration | Certificate Configuration**.

Support for Network Audit Tool

The Network Audit Tool in WEM supports the on demand or periodic auditing of IMG configuration attributes (audit attributes) such as PPP MRU, Auth Sequence, Bulkstats Schema Needs Update, etc.

Web Element Manager Path

Click **Security | Configuration Audit | Query Information**.

Click **Security | Configuration Audit | Schedule**.

Click **Security | Configuration Audit | On Demand**.

Click **Security | Configuration Audit | Results**.

IPMP Configuration on WEM Server

IP Multipath (IPMP) configuration is now provided on WEM server.

IP Multipathing is a feature supported on Sun® Solaris® provided by Sun Microsystems. With IPMP, two or more NICs are dedicated for each network to which the host connects. Each interface is assigned a static “test” IP address, which is used to access the operational state of the interface. Each virtual IP address is assigned to an interface, though there may be more interfaces than virtual IP addresses, some of the interfaces being purely for standby purposes. When the failure of an interface is detected its virtual IP addresses are swapped to an operational interface in the group.

IMPORTANT

IPMP is a feature supported on Sun® Solaris® provided by Sun Microsystems. The configuration is included in *Section VI* of the *System Administration Guide: IP Services* from Sun Microsystems. For more information, refer to the Sun documentation

No separate license key required for this configuration.

For more information on configuration of this feature on WEM Servers, refer *WEM Installation and Administration Guide.*

CHAPTER 2
FAULT MANAGEMENT

This section contains additions and changes made to the fault management features available in Release 8.0 unless specifically designated as being in Release 8.1.

SNMP MIB Objects in Release 8.0

This section describes various MIB objects and alarms for 8.0.

Modified Objects

- starPDIFVpnId
- starPDIFSessCurrentIpv6Active
- starPDIFSessCurrentIPv6Dormant
- starPDIFSessCurrentIPv6Active
- starPDIFSessCurrentIPv4Dormant
- starChassisGroup
- starIPPoolType
- starSS7RdEntry
- starCardMode
- starPortType
- starSDHEntry
- starE1TribEntry
- starE1TribOperState
- starFractE1Trib
- starFractE1TribEntry
- starFractE1TribSlot
- starFractE1TribPort
- starFractE1TribPath
- starFractE1TribBundNum
- starFractE1TribTimeslots
- starGPRSLinkTable
- starGPRSLinkEntry
- starCongestion ResourceType

Obsoleted Objects

No obsolete objects for Release 8.0.

New Objects

- starSCTPSelfPort
- starSCTPPeerPort
- starBLFilename
- starBLErrorCode
- starDiameterECode
- starIPMSServerTable
- starIPMSServerEntry
- starIPMSServerVpnId
- starIPMSServerAddr
- starIPMSServerVpnName
- starCertTable
- starCertEntry
- starCertSerialNumber
- starCertExpiryTime
- starentGPRSLink
- starGPRSEntry
- StarGPRSEntry
- starGPRSNsei
- starGPRSNsvci
- starGPRSBvci
- starDiameterEncoderString
- starSDHPathTable
- starSDHPathEntry
- starSDHPathSlot
- starSDHPathPort
- starSDHPathNum
- starSDHOperState
- starSDHPathOperState
- starE1TribTug2
- starE1TribTu12
- starE1TribOperStateLOP
- starFractE1TribTug2
- starFractE1TribTu12

Deleted Objects

- Starslotentry
- starSlotPartNumber

- starSlotPartRevision
- starSlotSerialNumber
- starSlotCLEICode
- starDiameterPeerAddrIpv6
- starBLFilename
- starBLErrorCode
- Star Chassis Group:
- starSlotPartNumber
- starSlotPartRevision,
- tarSlotSerialNumber,
- starSlotCLEICode,
- starDiameterPeerAddrIpv6,
- starDiameterIPv6PeerDown
- starSS7RdEntry
- starentIPMSServer
- starIPMSServerTabl
- starSDHOperStateSCT
- starSDHOperStateHOP
- starSDHOperStateLOP
- starSDHOperstatePath
- starE1TribNum
- starFractE1TribNum
- starSDHUp
- starSDHDown
- starE1TributoryDown

Modified Alarms

- starTrapGroup
- starM3UAPCUnavailable
- starSCTPAssociationFail
- starSCTPAssociationEstablished
- starSCTPPathDown
- starSCTPPathUp
- starTrapGroup

Obsoleted Alarms

No alarms were obsoleted in Release 8.0.

New Alarms

- starThreshFWDosAttack
- starThreshClearFWDosAttack
- starThreshFWDropPacket
- starThreshClearFWDropPacket
- starThreshFWDenyRule
- starThreshClearFWDenyRule
- starThreshFWNoRule
- starThreshClearFWNoRule
- starBSReachable
- starBSUnreachable
- starSystemStartup
- starSCCPSspRcvd
- starSCCPSspClear
- starSGSNRNCReset
- starSGSNHLRReset
- starSGSNGtpcPathFailure
- starSGSNGtpcPathFailureClear
- starSGSNGtpuPathFailure
- starSGSNGtpuPathFailureClear
- starMTP3LinkOutOfService
- starMTP3LinkInService
- starMTP3LinkSetUnAvailable
- starMTP3LinkSetAvailable
- starSCTPAssociationFail
- starSCTPAssociationEstablished
- starSCTPPathDown
- starSCTPPathUp
- starM3UAPSDown
- starM3UAPSPDown
- starM3UAPSActive
- starM3UAPSPUp
- starMTP3PCUnavailable
- starMTP3PCAvailable
- starSS7PCUnavailable
- starSS7PCAvailable
- starSS7PCCongested
- starSS7PCCongestionCleared

- starGPRSServiceStart
- starGPRSServiceStop
- starGPRSNseDown
- starGPRSNseUp
- starGPRSNsvcDown
- starGPRSNsvcUp
- starGPRSBvcDown
- starGPRSBvcUp
- starSDHSectionDown
- starSDHSectionUp
- starSDHPathHopDown
- starSDHPathHopUp
- starSDHLopDown
- starSDHLopUp
- starSDHE1TribDown
- starSDHE1TribUp
- starSDHFractE1LMIDown
- starSDHFractE1LMIup
- starM3UAPSPCongested
- starM3UAPSPCongestionCleared

Deleted Alarms

- starM3UAASDown
- starM3UAASActive
- starM3UAASPDown
- starM3UAASPUp
- starBLDBError
- starBLDBErrorClear
- starASNPCServiceStart
- starSDHDown
- starSDHUp
- starE1TributoryDown
- starE1TributoryUp
- starFractE1LMIDown
- starFractE1LMIUp

Web Element Manager Path

Select Configuration | SNMP Configuration.

SNMP MIB Objects in Release 8.1

Modified Objects

- starPortType
- starSGTPSerEntry
- starChassisGroup
- starMTP3LinkSetId
- StarChassisGroup
- starWindowTime
- starServiceSubLimit
- starTaskFacility
- starTaskCard
- starTaskInstance
- starTaskCPU
- starThreshInt
- starThreshMB
- starThreshGB
- starLicensedSessions
- starSS7RdEntry
- starSS7rdid
- starM3UAPsId
- starM3UAPspid
- starMTP3LinkSetId
- MTP3LinkId
- starSCTPSelfAddr
- starSCTPPeerAddr
- starSCTPSelfPort
- starSCTPPeerPort
- starChassisGroup
- StarTrapGroup
- starSessSub1AccessTech
- starSDHEntry
- starE1TribEntry
- starE1TribOperState
- starFractE1TribEntry
- starFractE1TribSlot
- starFractE1TribBundNum
- starFractE1TribTimeslots

- starcfcdpnotifgroup
- starcfmdbnotifgroup
- starCongestionResourceType
- starGPRSLinkEntry

Obsoleted Objects

No obsoleted objects for this release.

New Objects

- starDiameterPeerAddripv6
- starBLFileName
- starBLErrorCode
- starSGTPSelfPort
- starSGTPPeerPort
- starCertIssuer
- starFileEntry
- starFileTable
- starFileApplication
- starFileName
- starFTPServTable
- starFTPServEntry
- starFTPServVpnId
- starFTPServIpAddr;
- starFTPServVpnName
- starSlotPartNumber
- starSlotPartRevision
- starSlotSerialNumber
- starSlotCLEICode
- starCSCFPeerServerTable
- starCSCFPeerServerSvcID
- starCSCFPeerServerVpnID
- starCSCFPeerServerVpnName
- starCSCFPeerServerSvcName
- starCSCFPeerServerListName
- starThreshGPRSSessions
- starThreshClearGPRSSessions
- starThreshPerServiceGPRSSessions
- starThreshClearPerServiceGPRSSessions

- starThreshGPRSPdpSessions
- starThreshClearGPRSPdpSessions
- starThreshPerServiceGPRSPdpSessions
- starThreshClearPerServiceGPRSPdpSessions
- starSDHSlot
- starSDHPort
- StarSDHEntry
- starSDHOperState
- StarSDHTable
- starSDHOperstateHop
- StarSDHOperStateLop
- starSDHOperStatePath
- StarE1TribTable
- StarE1TribEntry
- StarE1TribSlot
- StarE1TribPort
- StarE1tribPath
- starE1TribNum
- StarE1TribOperState
- starFractE1Trib Table
- StarFractE1TribEntry
- StarFractE1TribSlot
- StarFractE1TribPort
- TribFractTribEntry
- StarFractE1TribNum
- StarFractE1TribBundNum
- StarFractE1TribTimeslots
- starFractE1TribBundNum
- starSDHOperStateSCT
- starSDHOperStateHOP
- starSDHoperStateLOP
- starSDHOperStatePath
- starSDHPathTable
- starSDHPathEntry
- starSDHPathSlot
- starSDHPathPort
- starSDHPathNum
- starSDHOperState

- starSDHPathOperState
- starE1TribTug2
- starE1TribTu12
- starE1TribOperStateLOP
- starFractE1TribTu12
- starLessMountPoint
- starStorageTable
- starStorageEntry
- starStorageName
- starStorageSlot
- starStorageDeviceType
- starGSSCDRLossConfigured
- starGSSCDRLossMeasured
- starStorageServerCDRLoss

Deleted Objects

- starSDHOperStateSCT
- starSDHOperstateHOP
- starSDHOperStateLOP
- starSDHOperStatePath
- starE1TribNum
- starFractE1TribNum
- CSCFPEERServer
- CSCFPeerServerTable
- CSCFPeerServerEntry
- CSCFPEERServerVpnID
- CSCFPEERServerVpnName
- CSCFPeerServerListName

Modified Alarms

- starSGSNGtpcPathFailure
- starSGSNGtpcPathFailureClear
- starSGSNGtpuPathFailure
- starSGSNGtpuPathFailureClear
- starSlotPartNumber
- starSlotPartRevision
- starSlotSerialNumber
- starcfmdbprocstart
- starcfmdbprocstop
- starcfmdbprocdbabsent
- starcfmdbprocapifailed
- starCfMdbProcDbParseError
- starcfcdpstart
- starcfmdbProcDbParseError
- starcfcdpstart
- starcfcdpstop
- starcfcdpRestart
- starcfCdpApiOpFailed
- starCfCdpThreshCPUUtilization
- starCfCdpClearThreshCPUUtilization
- starCfCdpThreshDiskUtilization
- starCfCdpClearThreshDiskUtilization
- starCfCdpThreshSwapUtilization
- starCfRestart
- starCfRestop
- starCfReRestart
- starCfReFileParsingAborted
- starCfReThreshCPUUtilization
- starCfReClearThreshCPUUtilization
- starCfReThreshDiskUtilization
- starCfReClearThreshDiskUtilization
- starCfDbThreshCPUUtilization
- starCfDbClearThreshCPUUtilization
- starCfDbThreshDiskUtilization
- starCfDbClearThreshDiskUtilization
- starCfCciApplicationStart
- starCfCciApplicationStop

- starThreshStorageUtilization
- starThreshClearStorageUtilization

Obsoleted Alarms

No alarms were obsoleted in Release 8.1.

New Alarms

- starBLDBError
- starBLDBErrorClear
- starASNPCServiceStart
- starASNPCServiceStop
- starDiameterCapabilitiesExchangeSuccess
- starDiameterCapabilitiesExchangeFailure
- starSRPConnDown
- starSRPConnUP
- starDiameterIPv6PeerDown
- starDiameterIpv6PeerUp
- starIPMSServerUnreachable
- starIPMSServerReachable
- starCertShortLifetime
- starCertExpired
- starCertValid
- starFTPPushFail
- starFTPServSwitch
- starFTPServSwith
- starSDHDown
- starSDHUp
- starE1TributaryDown
- starE1TributaryUp
- starFractE1LMIDown
- starFractE1LMIUp
- starFractE1TribEntry
- starFractE1LMITribSlot
- starFractE1LMITrib port
- starThreshASNGWSessions
- starThreshClearASNGWSessions
- starThreshPerServiceASNGWSessions
- starThreshClearPerServiceASNGWSessions

- starSDHPathHopDown
- starSDHPathHopUp
- starSDHFractE1LMIUp
- starSDHFractE1LMIDown
- starSDHSectionDown
- starSDHSectionUp
- starSDHe1TribDown
- starSDHE1TribUp
- starStorageFailed
- starRaidFailed
- starRaidStarted
- starRaidDegraded
- starRaidRecovered

Deleted Alarms

- starContFiltCFST16DBFailClear
- starContFiltCFST16DBFail
- starE1TributaryDown
- starE1TributaryUp
- starFractE1LMIUp
- starFractE1LMIDown
- starSDHDown
- starSDHUp

SNMP MIB Objects in Release 8.3

Modified Objects

There are no modified objects in the Release 8.3.

Obsoleted Objects

No obsoleted objects in the Release 8.3.

New Objects

- starLESSNotifRaisedTime
- starLESSNotifInfo
- starLESSInstance
- starLESSNodeName
- starLESSApplicationType
- starLESSThreshInt
- starLESSThreshMeasuredInt
- starLESSRuleBaseName
- starLESSSTXName
- starLESSStartofMissedRange
- starLESSEndofMissedRange
- starLESSFileType
- starLESSRemoteHostName
- starLessMountPoint
- starLESSApplicationStart
- starLESSApplicationReStart
- starLESSApplicationStop
- starLESSApplicationTerminated
- starLESSPullIntervalMissed
- starLESSThreshDiskUsage
- starLESSThreshClearDiskUsage
- starLESSFileMissed
- starLESSRemoteConnectionFail
- starLESSRemoteConnectionEstablished
- starLESSFileTransferFail
- starLESSFileTransferComplete
- starLESSThreshPendingFiles
- starLESSThreshClearPendingFiles

- starLESSNewHostFound
- starLESSHostRemoved
- starLESSMIBCompliance
- starLESSNotifMgmtGroup
- starLESSNotifGroup

Deleted Objects

There are no deleted objects for the Release 8.3.

Obsoleted Alarms

No alarms were obsoleted in Release 8.3.

New Alarms

- starThreshNAPTPortChunks
- starThreshClearNAPTPortChunks

Deleted Alarms

There are no deleted alarms in the Release 8.3.

Content Filtering MIB Objects for Release 8.0

This section contains new and modified MIB objects and alarms.

Modified Objects

No objects were modified in Release 8.0.

Obsolete Objects

No objects were obsoleted in Release 8.0.

New Objects

- starCfMdbProcMemUsageOverLimit
- starCfMdbProcMemUsageNormal
- starCfMdbProcCpuUsageOverLimit
- starCfMdbProcCpuUsageNormal
- starCfMdbProcDiskUsageOverLimit
- starCfMdbProcDiskUsageNormal
- starCfCdpApiVerError
- starCFMDBNotifGroup
- starCFCDPNotifGroup
- starCfEmsMcrdbsHostAddress
- starCfEmsDbType
- starCfEmsSourceDbFileName
- starCfEmsFromDbType
- starCfEmsToDbType
- starCfEmsDestDbFileName
- starCfEmsFtpHostInfo
- starCFCOMMONMIBCompliance
- starCFEMSMIBCompliance
- starCFEMSNotifGroup

Deleted Objects

No objects were deleted in Release 8.0.

Modified Alarms

No alarms were modified in Release 8.0.

Obsolete Alarms

- No alarms were obsoleted in Release 8.0.

New Alarms

- starCfEmsServerProcStart
- starCfEmsServerProcStop
- starCfEmsDbImportFailed
- starCfEmsDbImportSucceeded
- starCfEmsDbExportFailed
- starCFEMSDbExportSucceeded
- starCfEmsDbConversionFailed
- starCfEmsDbConversionSucceeded
- starCfEmsFtpConnectionFailed

Deleted Alarms

No alarms were deleted in Release 8.0.

Web Element Manager Path

Select Configuration | SNMP Configuration.

Content Filtering MIB Objects for Release 8.1

This section contains new and modified MIB objects and alarms.

Modified Objects

- starCFIpAddr.

Obsolete Objects

No objects were obsoleted in Release 8.1.

New Objects

- starCFMDBNotifMgmtGroup
- starCFCDPNotifMgmtGroup
- starCFRENotifMgmtGroup

Deleted Objects

- starCfEmsMcrdbsHostAddress
- starCfEmsDbType
- starCfEmsSourceDbFileName
- starCfEmsCdpHostAddress
- starCfEmsFromDbType
- starCfEmsToDbType
- starCfEmsDestDbFileName
- starCfEmsFtpHostInfo
- starCFEMSNotifMgmtGroup
- starCFEMSNotifGroup

Modified Alarms

- starCFEMSMIBCompliance

Obsolete Alarms

No alarms were obsoleted from Release 8.1.

New Alarms

- starCfCdpStart,
- starCfCdpStop,

- starCfCdpRestart,
- starCfCdpApiOpFailed,
- starCfCdpApiVerError,
- starCfCdpThreshCPUUtilization,
- starCfCdpClearThreshCPUUtilization,
- starCfCdpThreshDiskUtilization,
- starCfCdpClearThreshDiskUtilization,
- starCfCdpThreshSwapUtilization,
- starCfCdpClearThreshSwapUtilization,
- starCfCdpProcReportErrWithMsg,
- StarCfCdpProcApiCfdcmErrWithMsg
- starCfCdpProcApiPermissionDenied,
- starCfCdpProcApiInvalidAgrs,
- starCfReStart,
- starCfReStop,
- starCfReRestart,
- starCfReFileParsingAborted,
- starCfReThreshCPUUtilization,
- starCfReClearThreshCPUUtilization,
- starCfReThreshDiskUtilization,
- starCfReClearThreshDiskUtilization,
- starCfDbThreshCPUUtilization,
- starCfDbClearThreshCPUUtilization,
- starCfDbThreshDiskUtilization,
- starCfDbClearThreshDiskUtilization
- starCfCciApplicationStart,
- starCfCciApplicationStop,
- starCfCciCdpServerReachable,
- starCfCciCdpServerUnreachable,
- starCfCciThreshCpuUtilization,
- starCfCciClearThreshCpuUtilization,
- starCfCciThreshMemoryUtilization,
- starCfCciClearThreshMemoryUtilization
- starCfMdbProcStart,
- starCfMdbProcStop,
- starCfMdbProcDbAbsent,
- starCfMdbProcApiOpFailed,
- starCfMdbProcDbParseError,

- starCfMdbProcMemUsageOverLimit
- starCfMdbProcMemUsageNormal,
- starCfMdbProcCpuUsageOverLimit,
- starCfMdbProcCpuUsageNormal,
- starCfMdbProcDiskUsageOverLimit,
- starCfMdbProcDiskUsageNormal,
- starCfMdbProcInvalidFileName,
- starCfMdbProcReportErrWithMsg,
- starCfMdbProcCfdcmErrWithMsg,
- starCfMdbProcMcrdbsErrWithMsg

Deleted Alarms

- starCfEmsServerProcStart
- starCfEmsServerProcStop
- starCfEmsDbImportFailed
- starCfEmsDbImportSucceeded
- starCfEmsDbExportFailed
- starCFEMSDbExportSucceeded
- starCfEmsDbConversionFailed
- starCfEmsDbConversionSucceeded
- starCfEmsFtpConnetionFailed
- starCfEMSMIBCompliances

Content Filtering MIB Objects for Release 8.3

This section contains new and modified MIB objects and alarms.

Modified Objects

No objects were modified in Release 8.3.

Obsolete Objects

No objects were obsoleted in Release 8.3.

New Objects

- starCfEmsCdpHostAddress
- starCfEmsFromDbType
- starCfEmsDestDbFileName
- starCfEmsCdpHostAddress
- starCfEmsFromDbType
- starCfEmsToDbType
- starCfEmsDestDbFileName
- starCfEmsFtpHostInfo
- starCFEMSNotifMgmtGroup

Deleted Objects

No Objects were deleted in Release 8.3

Modified Alarms

No objects were modified in Release 8.3

Obsolete Alarms

No alarms were obsoleted from Release 8.3.

New Alarms

- starCfEmsServerProcStop
- starCfEmsDbImportFailed
- starCfEmsDbImportSucceeded
- starCfEmsDbExportFailed
- starCFEMSDbExportSucceeded

- starCfEmsDbConversionFailed
- starCfEmsDbConversionSucceeded
- starCfEmsFtpConnetionFailed
- starCFEMSNotifGroup

Deleted Alarms

No alarms were deleted form 8.3

ESS MIB Objects for Release 8.0

This section contains new and modified MIB objects and alarms pertaining to Local-External Storage Server (L-ESS).

Modified Objects

No objects were modified in Release 8.0.

Obsolete Objects

No objects were obsoleted in Release 8.0.

New Objects

No new objects were added in Release 8.0.

Deleted Objects

No objects were deleted for Release 8.0.

Modified Alarms

No alarms were modified in Release 8.0.

Obsolete Alarms

No alarms were obsoleted for Release 8.0.

New Alarms

No new alarms were added in Release 8.0.

Deleted Alarms

No alarms were deleted for Release 8.0.

ESS MIB Objects for Release 8.1

This section contains new and modified MIB objects and alarms pertaining to Local-External Storage Server (L-ESS).

Modified Objects

No objects were modified in Release 8.1.

Obsolete Objects

No objects were obsoleted in Release 8.1.

New Objects

The following objects are new for Release 8.1.

- starLESSFileType
- starLESSRemoteHostName

Deleted Objects

No objects were deleted for Release 8.1.

Modified Alarms

No alarms were modified in Release 8.1.

Obsolete Alarms

No alarms were obsoleted for Release 8.1.

New Alarms

The following alarms are new for Release 8.1.

- starLESSRemoteConnectionFail
- starLESSRemoteConnectionEstablished
- starLESSFileTransferFail
- starLESSFileTransferComplete
- starLESSThreshPendingFiles
- starLESSThreshClearPendingFiles
- starLESSNewHostFound
- starLESSHostRemoved

Deleted Alarms

No alarms were deleted for Release 8.1.

Intelligent Packet Monitoring Systems (IPMS) MIB in Release 8.1

This section contains new and modified MIB objects and alarms for IPMS in Release 8.1.

IMPORTANT

This is a new external application and available from Release 8.1 onward only. Refer *IPMS MIB* chapter of *SNMP MIB Reference*.

New Objects

- starIPMSTimeTicks
- starIPMSComponentName
- starIPMSTaskInfo
- starIPMSProcessMaxRestartCnt
- starIPMSProcessRestartWaitTime
- starIPMSPacketLossCnt
- starIPMSTotalPacketLossCnt
- starIPMSDPIFailureReason
- starIPMSDPIDetails
- starIPMSEventSource
- starIPMSAttribute
- starIPMSResourceType
- starIPMSResourceInfoState
- starIPMSResourceCurrentValue
- starIPMSResourceConfThreshold
- starIPMSPeerName
- starIPMSPeerIP
- starIPMSPeerPort
- starIPMSICMPState
- starIPMSCORBAState

Modified Objects

No objects were obsoleted in Release 8.1.

Obsolete Objects

No objects were obsoleted in Release 8.1.

New Alarms

- starIPMSComponentStart
- starIPMSComponentStop
- starIPMSProcessStart
- starIPMSProcessStartFail
- starIPMSPacketLossThreshold
- starIPMSDPIFail
- starIPMSThresholdExceed
- starIPMSThresholdClear
- starIPMSPeerStateChange

Modified Alarms

No alarms were modified in Release 8.1.

Obsolete Alarms

No alarms were obsoleted in Release 8.1.

Web Element Manager Path

Select Configuration | SNMP Configuration.

Web Element Manager Enhancements in Release 8.0

This section contains new and modified MIB objects and alarms for Web Element Manager. in Release 8.0.

New Objects

No new objects in Release 8.0.

Modified Objects

No objects were modified in Release 8.0.

Obsolete Objects

No objects were obsoleted in Release 8.0.

New Alarms

No new alarms in Release 8.0.

Modified Alarms

No alarms were modified in Release 8.0.

Obsolete Alarms

No alarms were obsoleted in Release 8.0.

Web Element Manager Path

Select Configuration | SNMP Configuration.

Web Element Manager Enhancements in Release 8.1

This section contains new and modified MIB objects and alarms for Web Element Manager. in Release 8.1.

New Objects

- starEMSCFMcrdbsHostAddress
- starEMSCFDbType
- starEmsCFSourceDbFileName
- starEMSCFCdpHostAddress
- starEMSCFFromDbType
- starEMSCFToDbType
- starEMSCFDestDbName
- starEMSBulkstatCounterValue
- starEMSCFFtpHostInfo

Modified Objects

- starEMSNotifMgmt
- starEmsNotifMgmtGroup

Obsolete Objects

No objects were obsoleted in Release 8.1.

New Alarms

- starEmsCFDBDirAccessible
- starEmsCFDBDirNonAccessible
- starEmsCFDBDirUsageOverLimit
- starEmsCFDBDirUsageNormal
- starEmsCFDbImportFailed
- starEmsCFDbImportSucceeded
- starEmsCFDbExportFailed
- starEmsCFDbExportSucceeded
- starEmsCFDbConversionFailed
- starEmsCFDbConversionSucceeded
- starEmsCFFtpConnetionFailed
- starEmsBulkStatCounterUsageOverLimit
- starEmsBulkStatCounterUsageNormal

Modified Alarms

No alarms were modified in Release 8.1.

Obsolete Alarms

No alarms were obsoleted in Release 8.1.

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 8.0 unless specifically designated as being in Release 8.1 or higher.

New Configuration Commands

Common Commands - New in Release 8.0

This section provides information on new commands that are common to products in Release 8.0.

aaa accounting-overload-protection

This command configures Overload Protection Policy for accounting requests.

CLI (Global Configuration Mode)

aaa accounting-overload-protection prioritize-gtpp
[default | no] aaa accounting-overload-protection

Web Element Manager Path

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

alarm-disable

The new command disables the alarm detection for designated sets of alarms on the Channelized line card.

CLI (Channelized Port Configuration Mode)

alarm-disable (all | ds1-e1 | none | sonet-sdh }

Web Element Manager Path

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

alarm-soak-timer

This command sets the timer for the duration that a detected alarm will be soaked before the alarm is reported.

CLI (Channelized Port Configuration Mode)

alarm-soak-timer *seconds*

Web Element Manager Path

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

card smc upgrade

This command upgrades programmables on the specified card. Must be followed by a slot number of card to upgrade.

CAUTION

This command should only be used if instructed by or working with Starent Support.

CLI (Exec Mode)

card smc upgrade *slot_number*

Web Element Manager Path

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

cdr

This command configures the CDR file transfer parameters. The following keywords are available with this command:

- **use-harddisk:** Specifies that the hard disk on the SMC be used to store EDR/UDR files. On configuring to use the hard disk for EDR/UDR storage, EDR/UDR files are transferred from RAMFS on the PSC card to the hard disk on the SMC card. Subsequently the files can be offloaded to an external server such as the L-ESS.

IMPORTANT

The **use-harddisk** keyword is only available on the ST40 platform.

- **push-interval value**: Specifies the transfer interval, in seconds, to push CDR files.
- **remove-file-after-transfer**: Specifies that the system is to remove an EDR/UDR file as soon as the file is pushed out of the system.
- **transfer-mode**: Specifies the CDR file transfer mode.

CLI (EDR Module Configuration Mode & UDR Module Configuration Mode)

cdr [push-interval *value* **| remove-file-after-transfer | transfer-mode { pull | push primary { encrypted-url** *enc_url* **| url** *url* **} [secondary { encrypted-secondary-url** *enc_sec_url* **| url** *sec_url* **}] } + | use-harddisk]**

no cdr [remove-file-after-transfer | use harddisk] +

default cdr [push-interval | remove-file-after-transfer | transfer-mode | use harddisk] +

Web Element Manager Path

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

cdr-push

This command initiates manual push of CDR files to the configured external storage server.

On ST16 chassis, this command must be run only from the context where the EDR/UDR module is configured. On ST40 chassis, this command must be run only from the local context. Running in other contexts will fail.

CLI (Exec Mode)

cdr-push { all | local-filename *file_name* **}**

Web Element Manager Path

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

context-timeout

Ensures that no expired contexts are used for data compression. Default is to 20 seconds. Replaces **context-cleanup-period** which has been obsoleted.

CLI (ROHC-Profile Decompress-Config Mode)

[default] context-timeout *seconds*

Web Element Manager Path

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

diameter send-ccri

This command configures sending CCR-I at the first user dcca-enabled-traffic detection, or on receiving Create-PDP-Context-Request.

CLI (Credit Control Configuration Mode)

diameter send-ccri { session-start | traffic-start }

default diameter send-ccri

Web Element Manager Path

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

flow-control

Flow control is enabled by default on the Quad-Gig-E (QGLC) line card. If flow control is not required, it can be disabled on a per-port basis using the **no** option.

CLI (Ethernet Port Config Mode)

[no] flow-control

Web Element Manager Path

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

frame-relay

This command defines the Frame Relay characteristics of the port.

CLI (Channelized Port Configuration Mode)

frame-relay path *path_id* **{ ds1** *connects* **| e1** *connects***} [timeslots |**
frame-relay [intf-type *intf_type* **[lmi_type** *lmi_type* **]]]**

Web Element Manager Path

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

header-type

This command sets the size of the header frame for a Frame Relay-type message emanating from a channelized line card.

CLI (Card Configuration Mode)

[default] header-type *header-size*

Web Element Manager Path

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

hopath-sdsf

This command defines the high-order path SDSF bit error rate (BER) threshold.

CLI (Channelized Port Configuration Mode)

hopath-sdsf *hopath_value*

Web Element Manager Path

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

hopath-sdsf

This command defines the high-order path SDSF bit error rate (BER) threshold.

CLI (Channelized Port Configuration Mode)

hopath-sdsf *hopath_value*

Web Element Manager Path

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

ingress-mode

This command toggles between enabling and disabling the port ingress mode.

CLI (Port Ethernet Configuration Mode)

ingress-mode

Web Element Manager Path

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

initial-e1-framing

With this keyword, the user has the option to choose the boot-time framing mode for all the E1s on the line card.

CLI (Card Configuration Mode Commands)

initial-e1-framing [crc4 | standard]

default initial-e1-framing

Web Element Manager Path

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

ipv6 access-list

A new command mode was added to configure IPv6 ACL commands.

CLI (Exec Mode Commands)

ipv6 access-list *name*

The following commands are included in this mode:

- deny/permit (any)

- deny/permit (by host IP address)
- deny/permit (by IP packets)
- deny/permit (by source ICMP packets)
- deny/permit (by source IP address masking)
- deny/permit (by TCP/UDP packets)
- end
- exit
- readdress server
- redirect context (any)
- redirect context (by host IP address)
- redirect context (by IP address masking)
- redirect context (by IP packets)
- redirect context (by source ICMP packets)
- redirect context (by TCP/UDP packets
- redirect css delivery-sequence (any)
- redirect css delivery-sequence (by host IP address)
- redirect css delivery-sequence (by IP address masking)
- redirect css delivery-sequence (by IP packets)
- redirect css delivery-sequence (by source ICMP packets)
- redirect css delivery-sequence (by TCP/UDP packets)
- redirect css service (any)
- redirect css service (by host IP address)
- redirect css service (by ICMP packets)
- redirect css service (by IP packets)
- redirect css service (by source IP address masking)
- redirect css service (by TCP/UDP packets)
- redirect css service (for downlink, any)
- redirect css service (for downlink, by host IP address)
- redirect css service (for downlink, by ICMP packets)
- redirect css service (for downlink, by IP packets)
- redirect css service (for downlink, by source IP address masking)
- redirect css service (for downlink, by TCP/UDP packets)
- redirect css service (for uplink, any)
- redirect css service (for uplink, by host IP address)
- redirect css service (for uplink, by ICMP packets)
- redirect css service (for uplink, by IP packets)
- redirect css service (for uplink, by source IP address masking)
- redirect css service (for uplink, by TCP/UDP packets)

- redirect nexthop (any)
- redirect nexthop (by host IP address)
- redirect nexthop (by IP address masking)
- redirect nexthop (by IP packets)
- redirect nexthop (by source ICMP packets)
- redirect nexthop (by TCP/UDP packets)

Web Element Manager Path

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

line-timing

This command instructs the system to recover the receive timing source from an external device via the optical (ATM) line card attached to the port.

CLI (ATM Port Configuration Mode)

`line-timing`

Web Element Manager Path

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

line-timing

This command instructs the system to recover the receive timing source from an external device via the channelized line card attached to the port.

CLI (Channelized Port Configuration Mode)

`line-timing`

Web Element Manager Path

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

link-aggregation

Link aggregation combines up to four ports on a redundant pair of Quad Gig-E line card so a large file is guaranteed to be sent serially down the same pipe rather than be distributed and be subject to massive packet re-ordering. LACP is the link aggregation control protocol.

CLI (Ethernet Port Config Mode)

`[ no ] link-aggregation { master | member } |` *`group N`* **`}`**
`[ lacp { active | passive } ] [ rate { slow | fast } ]`
`default link-aggregation lacp`

Web Element Manager Path

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

link-aggregation system-priority

Configures the link-aggregation system-priority hex value for a system, which comprises a PSC and its associated QGLC(s).

CLI (Card Config Mode)

link-aggregation system-priority *priority*

default link-aggregation system-priority

Web Element Manager Path

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

loopback

This command configures various loopback signals to troubleshoot the SDH/SONET physical layers.

CLI (Channelized Port Configuration Mode)

loopback { ds1-e1-diag | ds1-e1-line | none | sonet-sdh-diag | sonet-sdh-line }

Web Element Manager Path

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

lopath-sdsf

This command defines the low-order path SDSF bit error rate (BER) threshold.

CLI (Channelized Port Configuration Mode)

lopath-sdsf *lopath_value*

Web Element Manager Path

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

nai-construction

Creates a constructed-nai configuration on a per-APN basis only rather than by per-aaa-group.

CLI (APN Configuration Mode Commands)

nai-construction {imsi | msisdn} [override-null-username] [encrypted password *string* **| use-shared-secret-password | password** *string*]

no nai-construction

Web Element Manager Path

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

port bits

Using this command enters the BITS port configuration mode which provides configuration for the transmit timing source. The new BITS port configuration mode includes the following commands:

- default
- end
- exit
- mode
- no
- preferred slot
- recover
- shutdown
- snmp trap link-status

CLI (Global Configuration Mode)

port bits *slot#/port#***>**

Web Element Manager Path

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

radius accounting interim volume

This command configures the volume of uplink and downlink volume octet counts that triggers RADIUS interim accounting. This command is now available for PDSN and HA services.

CLI (AAA Server Group Configuration Mode & Context Configuration Mode)

radius accounting interim volume { downlink *bytes* **uplink** *bytes* **| total** *bytes* **| uplink** *bytes* **downlink** *bytes* **}**

no radius accounting interim volume

Web Element Manager Path

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

radius usage-reporting-algorithm

This command configures the usage reporting algorithm for RADIUS prepaid using DCCA.

CLI (Global Configuration Mode)

radius usage-reporting-algorithm { cumulative | relative }
default radius usage-reporting-algorithm

Web Element Manager Path

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

require detailed-rohc-stats

This command enables/disables detailed ROHC stats

CLI (Global Config Mode)

[no] require detailed-rohc-stats

Web Element Manager Path

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

require diameter-proxy

This command enables/disables Diameter Proxy mode.

CLI (Global Configuration Mode)

require diameter-proxy { multiple | single }
no require diameter-proxy

Web Element Manager Path

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

show timing

This command displays the information configured to define a transmit timing source other than the system clock. The display includes related information (such as port status, timing source priority, timing alarms, etc.) for all of the ports configured for either BITS or line timing.

CLI (Exec Mode)

show timing

Web Element Manager Path

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

toh-sdsf

This command defines the line SDSF bit error rate (BER) threshold for a port on a Channelized line card.

CLI (Channelized Port Configuration Mode)

toh-sdsf *toh_value*

Web Element Manager Path

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

use proxy

This command enables/disables Diameter proxy for the current endpoint.

CLI (Global Configuration Mode)

```
[ no ] use-proxy
```

Web Element Manager Path

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

Common Commands - New in Release 8.1

IMPORTANT

The new commands documented in this section are only available in Release 8.1.

card lc upgrade

This command upgrades programmables on the specified card. Must be followed by a slot number of card to upgrade.

CAUTION

This command should only be used if instructed by or working with Starent Support.

CLI (Exec Mode)

`card lc upgrade` *`slot_number`*

Web Element Manager Path

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

cea-timeout

This command configures the Capabilities-Exchange-Answer (CEA) message timeout duration for Diameter session.

CLI (Diameter Endpoint Configuration Mode)

`cea-timeout` *`duration`*
`default cea-timeout`

Web Element Manager Path

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

clear ipv6 neighbors

Clears the given ipv6 address from the neighbor cache.

CLI (Exec Mode)

`clear ipv6 neighbors` *`ipv6address`*

Web Element Manager Path

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

clock

New timezone **asia-azerbaijan** added for Baku (GMT+4:00; Baku, Azerbaijan)) to configure system clock on chassis.

CLI (Global Configuration Mode)

clock timezone *tz* **[local]**

no clock timezone

Web Element Manager Path

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

diameter request-timeout

This command configures the request-timeout setting for Diameter-IMSA Gx interface.

CLI (Policy Control Configuration Mode)

diameter request-timeout *timeout*

default diameter request-timeout

Web Element Manager Path

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

diameter sctp

This command configures Diameter SCTP parameters for all Diameter endpoints within the context.

CLI (Context Configuration Mode)

diameter sctp { hearbeat-interval *interval* **| path max-retransmissions** *retransmissions* **}**

default diameter sctp { heartbeat-interval | path max-retransmissions }

Web Element Manager Path

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

dpa-timeout

This command configures the Disconnect-Peer-Answer (DPA) message timeout duration for Diameter session.

CLI (Diameter Endpoint Configuration Mode)

dpa-timeout *duration*

default dpa-timeout

Web Element Manager Path

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

flow-control

Flow control is enabled by default on the Quad- Gig-E line card. If flow control is not required, it can be disabled on a per-port basis using the **no** option.

CLI (Ethernet Port Config Mode)

[no] flow-control

Web Element Manager Path

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

hd raid

A new command manages the RAID properties on the ST40 SMC hard disks when the hard disk controller task cannot automatically make the correct decisions or admin intervention is required by policy enforcement.

CLI (Exec Mode)

hd raid { check | create { *local1* **|** *remote1* **} | insert {** *local1* **|** *remote1* **} | overwrite {** *local1* **|** *remote1* **} | remove {** *local1* **|** *remote1* **} | select {** *local1* **|** *remote1* **} }**

hd raid

A new command accesses the HD RAID configuration mode which defines HD RAID management policies with the following commands:

- end
- exit
- overwrite
- select

CLI (Global Config Mode)

hd raid

Web Element Manager Path

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

idle-timeout-activity ignore-downlink

Allows a session idle-timeout to be reset with either uplink-only traffic or both uplink and downlink traffic. The default is **no idle-timeout-activity ignore-downlink**.

If **idle-timeout-activity ignore-downlink** is configured, the downlink traffic will not be used to reset the idle-timeout. Only uplink packets will be able to reset the idle-timeout. By default, **ignore-downlink** is negated by the **no** command so both uplink and downlink traffic is used to reset the idle-timeout.

CLI (APN Configuration Mode Commands)

[no] idle-timeout-activity ignore-downlink

default idle-timeout-activity

Web Element Manager Path

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

ikev1 disable-phase1-rekey

New command added to configure the rekeying of Phase1 SA when the Internet Security Association and Key Management Protocol (ISAKMP) lifetime expires in Internet Key Exchange (IKE) v1 protocol. This command replaced the **`isakmp disable-phase1-rekey`** command.

CLI (Context Configuration Mode)

`[ no ] ikev1 disable-phase1-rekey`

Web Element Manager Path

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

ikev1 keepalive dpd

New command added to configure the ISAKMP IPSec Dead Peer Detection (DPD) message parameters for IKE v1 protocol. This command replaced the **`isakmp keepalive`** command.

CLI (Context Configuration Mode)

`[ no ] ikev1 keepalive dpd interval` *`interval`* **`timeout`** *`time`* **`num-retry`** *`retries`*

Web Element Manager Path

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

ikev1 policy

New command added to configure/create an ISAKMP policy with the specified priority and enters ISAKMP Configuration Mode for IKE v1 protocol. This command replaced the **`isakmp policy`** command.

CLI (Context Configuration Mode)

`[ no ] ikev1 policy` *`priority`*

Web Element Manager Path

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

ipms

This command enables IPMS Client Configuration Mode for Intelligent Packet Monitoring System (IPMS) support on an AGW, configuring IPMS server connectivity in the context.

IMPORTANT

Currently this external application is available on PDIF service only. Client CLI (Context Configuration Mode)

`[ no ] ipms [-noconfirm ]`

Web Element Manager Path

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

ping6

Support is now provided to ping IPv6 addresses.

CLI (Exec Mode)

```
ping6 { hostname | ipv6 address }
```

Web Element Manager Path

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

service-type

This command configures the type of service (Frame Relay or pwe3-cse) to be employed on the CLC or CLC2 (channelized line cards).

CLI (Card Configuration Mode)

```
service-type { frame-relay | pwe3-cesopsn | unspecified }
default service-type
```

Web Element Manager Path

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

set control-dont-fragment

This command controls the don't fragment (DF) bit in the outer IP header of the IPsec tunnel data packet. It is a new keyword for the **`set`** command in the following crypto map configuration modes:

- ipsec-isakmp
- ipsec-ikev1
- ipsec-manual
- ipsec-dynamic
- ipsec-subscriber

It is also issued as **`control-dont-fragment`** (without the **`set`** command) in the crypto template configuration mode.

CLI (Crypto Map Config Mode)

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

CLI (Crypto Template Config Mode)

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

Options are:

- **`clear-bit`**: Clears the DF bit from the outer IP header (sets it to 0).
- **`copy-bit`**: Copies the DF bit from the inner IP header to the outer IP header. This is the default action.
- **`set-bit`**: Sets the DF bit in the outer IP header (sets it to 1).

Web Element Manager Path

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

single-port-mode

New command added in to enable/disable the he L2TP LAC service always to use standard L2TP port 1701 as source port for all L2TP control and data packets originated from LAC node.

CLI (LAC Service Configuration Mode)

```
[no | default] single-port-mode
```

Web Element Manager Path

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

tunnel selection-key

New command added in to support the creation of L2TP tunnels between LAC service on GGSN and an LNS server on the basis of attribute, “Tunnel-Server-Auth-ID”, value received from AAA server.

CLI (LAC Service Configuration Mode)

```
tunnel selection-key  { tunnel-server-auth-id | none }
[default] tunnel selection-key
```

Web Element Manager Path

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

IMPORTANT

Currently this feature is supported for GGSN only.

Common Commands - New in Release 8.3

This section provides information on new commands that are common to products in Release 8.3.

diameter mscc-per-ccr-update

This command configures sending single/multiple MSCC AVP (Multiple-Services-Credit-Control) in CCR-U messages.

CLI (Credit Control Configuration Mode)

```
diameter mscc-per-ccr-update { multiple | single }

default diameter mscc-per-ccr-update
```

Web Element Manager Path

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

CF Commands - New in Release 8.0

This section provides information on new commands available in Release 8.0.

failure-action

This command specifies the action to be taken when communication between ICAP endpoints within a Content Filtering Server Group fails. This command replaces the **`timeout action`** command.

CLI (Content Filtering Server Group Configuration Mode)

`failure-action { allow | content-insertion` *`content_string`* **`| discard | redirect-url`** *`url`* **`| terminate-flow }`**

`[ default | no ] failure-action`

Web Element Manager Path

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

CF Commands - New in Release 8.1

IMPORTANT

The new commands documented in this section are only available in Release 8.1.

content-filtering category match-method

This command sets the match method to look up URLs in the category-based content filtering database.

CLI (ACS Configuration Mode)

content-filtering category match-method { exact | generic }
default content-filtering category match-method

Web Element Manager Path

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

content-filtering flow-any-error

This command configures allowing/discarding of Content Filtering packets in case of ACS error scenarios.

CLI (Rulebase Configuration Mode)

content-filtering flow-any-error { deny | permit }
default content-filtering flow-any-error

Web Element Manager Path

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

discarded-flow-content-id

This command is used in the configuration to account for packets discarded as a result of Content Filtering action.

CLI (Content Filtering Policy Configuration Mode)

discarded-flow-content-id *content_id*
no discarded-flow-content-id

Web Element Manager Path

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

failure-action

This command specifies the failure action when the content filtering analysis results are not available to analyze.

CLI (Content Filtering Policy Configuration Mode)

failure-action { allow | content-insert *content_string* **| discard | redirect-url** *url* **| terminate-flow | www-reply-code-and-terminate-flow** *reply_code* **} [edr** *edr_format_name* **]**
default failure-action [edr *edr_format_name* **]**

Web Element Manager Path

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

upgrade url-blacklisting database

This command upgrades and loads URL Blacklisting database on the ACSMgrs.

CLI (Exec Mode)

upgrade url-blacklisting database [-noconfirm]

Web Element Manager Path

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

url-blacklisting action

This command enables/disables URL Blacklisting functionality for the rulebase, and configures the EDRs to be generated on Blacklisting match and the action to take.

CLI (Rulebase Configuration Mode)

url-blacklisting action { discard | redirect-url *url* **| terminate-flow | www-reply-code-and-terminate-flow** *reply_code* **} [edr** *edr_format_name* **]**

[default | no] url-blacklisting action

Web Element Manager Path

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

url-blacklisting database

This command configures URL Blacklisting database directory parameters.

CLI (Global Configuration Mode)

url-blacklisting database { directory path *path* **| max-versions** *max_versions* **| override file** *file_name* **}**

default url-blacklisting database { directory path | max-versions | override file }

Web Element Manager Path

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

url-blacklisting match-method

This command sets the match method to look up URLs in the URL Blacklisting database.

CLI (ACS Configuration Mode)

url-blacklisting match-method { exact | generic }

default url-blacklisting match-method

Web Element Manager Path

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

ECS Commands - New in Release 8.0

This section provides information on new commands available in Release 8.0.

add-ruledef

This command adds a ruledef to the current Group of Ruledefs.

CLI (Group of Ruledefs Configuration Mode)

add-ruledef priority *priority* **ruledef** *ruledef_name*
no add-ruledef priority *priority*

Web Element Manager Path

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

group-of-ruledefs

This command creates a group of rule definitions, and enters the Group-of-Ruledefs configuration mode.

CLI (ACS Configuration Mode)

group-of-ruledefs *ruledef_group* **[- noconfirm]**
no group-of-ruledefs *ruledef_group*

The Group-of-Ruledefs configuration mode was added. The following commands are available in this mode:

- **add-ruledef**
- **end**
- **exit**
- **no**

Web Element Manager Path

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

host-pool

This command creates a host pool, and enters the ACS Host Pool Configuration mode.

CLI (ACS Configuration Mode)

[no] host-pool *host_pool* **[- noconfirm]**

Web Element Manager Path

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

http error

This command defines a rule definition to analyze user traffic for invalid HTTP packets and other errors while parsing HTTP packets.

CLI (Ruledef Configuration Mode)

[no] http error *operator condition*

Web Element Manager Path

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

idle-timeout

This command specifies the maximum duration a flow type can remain idle, in seconds, after which the system automatically terminates the flow.

CLI (ACS Configuration Mode)

idle-timeout { icmp | tcp | udp } *idle_duration*

[default | no] idle-timeout { icmp | tcp | udp }

Web Element Manager Path

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

imsi-pool

This command creates an IMSI pool, and enters the ACS IMSI Pool Configuration mode.

CLI (ACS Configuration Mode)

[no] imsi-pool *imsi_pool* **[- noconfirm]**

Web Element Manager Path

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

ip error

This command defines a rule definition to analyze user traffic for invalid IP packets and other errors while parsing IP packets.

CLI (Ruledef Configuration Mode)

[no] ip error *operator condition*

Web Element Manager Path

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

ip max-fragments

This command limits the maximum number of IP fragments per fragment chain.

CLI (ACS Configuration Mode)

ip max-fragments *max_fragments*

default ip max-fragments

Web Element Manager Path

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

ip reset-tos

This command configures the system to be able to reset the IP Type of Service (ToS).

CLI (Rulebase Configuration Mode)

ip tos-reset
default ip tos-reset
no ip tos-reset

Web Element Manager Path

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

ip vlan

This command configures the VLAN identifier to be associated with the IP address for the session.

CLI (Charging Action Configuration Mode)

ip vlan *range*
[default | no] ip vlan

Web Element Manager Path

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

nexthop-forwarding-address

This command configures the next-hop forwarding address for a charging action.

CLI (Charging Action Configuration Mode)

nexthop-forwarding-address *ipv4_address*
no nexthop-forwarding-address

Web Element Manager Path

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

packet-filter

This command creates an Active Charging Service Packet Filter, and enters the Packet Filter Configuration mode.

CLI (ACS Configuration Mode)

packet-filter *filter_name* **[-noconfirm]**
no packet-filter *filter_name*

Web Element Manager Path

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

port-map

This command creates a port map, and enters the ACS Port Map Configuration mode.

CLI (ACS Configuration Mode)

[no] port-map *port_map* **[- noconfirm]**

Web Element Manager Path

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

qos-class-identifier

This command configures the QoS Class Identifier.

CLI (Charging Action Configuration Mode)

qos-class-identifier *identifier*

no qos-class-identifier

Web Element Manager Path

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

qos-renegotiate traffic-class

This command configures the QoS traffic class for the charging action for the Layer 7 QoS Renegotiation feature, enabling triggering QoS renegotiation from an active-charging rule. This command is controlled by the dynamic-qos-renegotiation license.

CLI (Charging Action Configuration Mode)

qos-renegotiate traffic-class { background | conversational | interactive *priority* **| streaming }**

no qos-renegotiate

Web Element Manager Path

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

qos-renegotiate timeout

This command configures the timeout setting for the Quality of Service (QoS) Renegotiation feature. This command is controlled by the dynamic-qos-renegotiation license.

CLI (Rulebase Configuration Mode)

qos-renegotiate timeout *timeout*

no qos-renegotiate timeout

Web Element Manager Path

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

rtcp uri

This command defines a rule definition to analyze and charge user traffic using Uniform Resource Identifier (URI) associated with Real-time Transport Control Protocol (RTCP).

CLI (Ruledef Configuration Mode)

[no] rtp uri [case-sensitive] operator string

Web Element Manager Path

Click Configuration | Active Charging | Active Charging Service and click **Add** or **Modify**.

tcp check-window-size

This command enables/disables TCP window-size checking.

CLI (Rulebase Configuration Mode)

[default | no] tcp check-window-size

Web Element Manager Path

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

tcp packets-out-of-order

This command configures the options for out-of-order packets.

CLI (Rulebase Configuration Mode)

tcp packets-out-of-order { timeout *duration_ms* **| transmit [after-reordering | immediately] }**

default tcp packets-out-of-order { timeout | transmit }

Web Element Manager Path

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

tft packet-filter

This command configures the packet filter to be sent to the MS.

CLI (Charging Action Configuration Mode)

[no] tft packet-filter *packet_filter*

Web Element Manager Path

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

url-extraction

This command enables configuration of ICAP URL extraction behavior.

CLI (Content Filtering Server Group Configuration Mode)

url-extraction { after-parsing | raw }

default url-extraction

Web Element Manager Path

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

wtp packets-out-of-order

This command configures how to process TCP packets that are out of order, while waiting for the earlier packet(s) to arrive.

CLI (Rulebase Configuration Mode)

wtp packets-out-of-order { out-of-order-timeout *timeout* **| transmit [after-reordering | immediately] }**

default wtp packets-out-of-order { out-of-order-timeout | transmit }

Web Element Manager Path

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

ECS Commands - New in Release 8.1

This section provides information on new commands available in Release 8.1.

bearer 3gpp apn

This command defines a rule definition to analyze and charge user traffic based on APN of the bearer flow.

CLI (Ruledef Configuration Mode)

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

Web Element Manager Path

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

bearer 3gpp imsi

This command defines a rule definition to analyze and charge user traffic based on the International Mobile Station Identification number (IMSI) in bearer flow.

CLI (Ruledef Configuration Mode)

[no] bearer 3gpp imsi { *operator imsi* **| { !range | range } imsi-pool** *imsi_pool* **}**

Web Element Manager Path

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

bearer 3gpp rat-type

This command defines a rule definition to analyze and charge user traffic based on the Radio Access Technology (RAT) in bearer flow.

CLI (Ruledef Configuration Mode)

[no] bearer 3gpp rat-type *operator rat*

Web Element Manager Path

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

bearer 3gpp sgsn-address

This command defines a rule definition to analyze and charge user traffic based on SGSN address associated in bearer flow. This command replaces the **bearer sgsn-address** command.

CLI (Ruledef Configuration Mode)

[no] bearer 3gpp sgsn-address *operator address*

Web Element Manager Path

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

edr transaction-complete

This command configures the generation of an EDR on the completion of a transaction. In this release EDR generation is supported only for HTTP protocol.

CLI (Rulebase Configuration Mode)

edr transaction-complete http edr-format *edr_format*

{ default | no } edr transaction-complete

Web Element Manager Path

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

extract-host-from-uri

If the host field is not present in HTTP/WSP header, this command will extract host from URI, and store it in the host field.

CLI (Rulebase Configuration Mode)

extract-host-from-uri { http | wsp +)

{ default | no } extract-host-from-uri

Web Element Manager Path

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

http error

This command defines a rule definition to analyze user traffic for invalid HTTP packets and other errors while parsing HTTP packets.

CLI (Ruledef Configuration Mode)

[no] http error *operator condition*

Web Element Manager Path

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

ip error

This command defines a rule definition to analyze user traffic for invalid IP packets and other errors while parsing IP packets.

CLI (Ruledef Configuration Mode)

[no] ip error *operator condition*

Web Element Manager Path

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

rtp parent-proto

This command defines a rule definition to analyze and charge user traffic based on the parent protocol of the RTP flow.

CLI (Ruledef Configuration Mode)

[no] rtp parent-proto *operator parent_protocol*

Web Element Manager Path

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

rtcp parent-proto

This command defines a rule definition to analyze and charge user traffic based on the parent protocol of the RTCP flow.

CLI (Ruledef Configuration Mode)

[no] rtcp parent-proto *operator parent_protocol*

Web Element Manager Path

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

start

This command configures timeslots in a timedef.

CLI (Timedef Configuration Mode)

[no] start day { friday | monday | saturday | sunday | thursday | tuesday | wednesday } time *hh mm ss* **end day { friday | monday | saturday | sunday | thursday | tuesday | wednesday } time** *hh mm ss*

[no] start time *hh mm ss* **end time** *hh mm ss*

Web Element Manager Path

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

tcp check-window-size

This command enables/disables TCP window-size checking.

CLI (Rulebase Configuration Mode)

[default | no] tcp check-window-size

Web Element Manager Path

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

tcp mss

This command configures the TCP Maximum Segment Size (MSS) in TCP SYN packets.

CLI (Rulebase Configuration Mode)

tcp mss *tcp_mss* **{ add-if-not-present | limit-if-present } +**

[default | no] tcp mss

Web Element Manager Path

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

timedef

This command enables creating/configuring/deleting an ACS Time Definition (timedef) for the Time-of-Day Activation/Deactivation feature.

A new configuration mode “Timedef Configuration Mode” was added to configure the timedefs. The following commands are included in this mode:

- **end**
- **exit**
- **start**

CLI (ACS Configuration Mode)

timedef *timedef_name* **[-noconfirm]**

no timedef *timedef_name*

Web Element Manager Path

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

url-extraction

This command enables configuration of ICAP URL extraction behavior.

CLI (Content Filtering Server Group Configuration Mode)

url-extraction { after-parsing | raw }

default url-extraction

Web Element Manager Path

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

wsp x-header

This command defines a rule definition to analyze and charge user traffic based on WSP extension-headers (x-headers).

CLI (Ruledef Configuration Mode)

[no] wsp x-header *name* **[case-sensitive]** *operator string*

Web Element Manager Path

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

ECS Commands - New in Release 8.3

This section provides information on new commands available in Release 8.3.

post-processing priority

This command configures the post-processing action to be taken for the specified ruledef in the rulebase.

CLI (Rulebase Configuration Mode)

post-processing priority *priority* **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.

Firewall Commands - New in Release 8.0

This section provides information on new commands available in Release 8.0.

firewall dos-protection

This command configures firewall protection from Denial-of-Service (DoS) attacks.

CLI (ACS Configuration Mode)

[no] firewall dos-protection { all | flooding { icmp | tcp-syn | udp } | ftp-bounce | ip-unaligned-timestamp | mime-flood | seq-number-out-of-range | seq-number-prediction | source-router | teardrop | winnuke }

default firewall dos-protection

Web Element Manager Path

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

firewall flooding

This command configures firewall protection from packet flooding attacks.

CLI (ACS Configuration Mode)

firewall flooding { { protocol { icmp | tcp-syn | udp } packet limit *packets* **} | { sampling-interval** *interval* **} }**

default firewall flooding { { protocol { icmp | tcp-syn | udp } packet limit } | { sampling-interval } }

Web Element Manager Path

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

firewall max-ip-packet-size

This command configures the maximum IP packet size allowed over firewall.

CLI (ACS Configuration Mode)

firewall max-ip-packet-size *packet_size* **protocol { icmp | non-icmp }**

default firewall max-ip-packet-size protocol { icmp | non-icmp }

Web Element Manager Path

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

firewall mime-flood

This command configures firewall protection from mime-flood attacks.

CLI (ACS Configuration Mode)

firewall mime-flood { http-headers-limit *max_limit* **| max-http-header-field-size** *max_size* **}**

default firewall mime-flood { http-headers-limit | max-http-header-field-size }

Web Element Manager Path

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

firewall priority

This command adds and specifies the priority of a firewall rule definition in the rulebase, and allows to configure a single or range of ports to be allowed on the server for auxiliary/data connections.

CLI (Rulebase Configuration Mode)

firewall priority *priority* **firewall-ruledef** *ruledef_name* **{ { permit [trigger open-port {** *aux_port_number* **| range** *start_port_number* **to** *end_port_number* **} direction { both | reverse | same }] } | { deny [charging-action** *charging_action* **] } }**

no firewall priority *priority*

Web Element Manager Path

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

firewall ruledef

This command creates a Firewall Ruledef, and enters the ACS Firewall Ruledef Configuration Mode.

CLI (ACS Configuration Mode)

[no] firewall ruledef *ruledef_name* **[-noconfirm]**

Web Element Manager Path

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

firewall tcp-syn-flood-intercept

This command enables and configures the TCP intercept parameters to prevent TCP SYN flooding attacks by intercepting and validating TCP connection requests for DoS protection mechanism configured with the **dos-protection** command.

CLI (ACS Configuration Mode)

firewall tcp-syn-flood-intercept { max-attempts *max_attempts* **| mode { none | { intercept | watch } [aggressive] } | retransmit-timeout** *retransmit_timeout* **| watch-timeout** *intercept_watch_timeout* **}**

default firewall tcp-syn-flood-intercept { max-attempts | mode | retransmit-timeout | watch-timeout }

Web Element Manager Path

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

Firewall Commands - New in Release 8.1

IMPORTANT

The new commands documented in this section are only available in Release 8.1.

bearer username

This command defines firewall rule definition to analyze user traffic based on user name of the bearer flow.

CLI (ACS Firewall Ruledef Configuration Mode)

`[ no ] bearer username [ case-sensitive ]` *`operator value`*

Web Element Manager Path

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

firewall flow-recovery

This command configures Firewall flow recovery parameters.

CLI (ACS Configuration Mode)

`firewall flow-recovery { downlink | uplink } [ timeout` *`timeout`* **`]`**
`{ default | no } firewall flow-recovery { downlink | uplink }`

Web Element Manager Path

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

firewall icmp-destination-unreachable-message-threshold

This command configures a threshold on the number of ICMP error messages sent by the subscriber for a particular data flow.

CLI (ACS Configuration Mode)

`firewall icmp-destination-unreachable-message-threshold` *`messages`*
`then-block-server`
`[ default | no ] firewall icmp-destination-unreachable-message -threshold`

Web Element Manager Path

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

firewall nat-alg

This command enables/disables the specified NAT Application Level Gateway (ALG).

CLI (ACS Configuration Mode)

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

Web Element Manager Path

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

firewall no-ruledef-matches

This command configures the default action for packets with no Firewall ruledef matches.

CLI (ACS Configuration Mode)

firewall no-ruledef-matches { downlink | uplink } action { deny [charging-action *charging_action* **] | permit }**

default firewall no-ruledef-matches { downlink | uplink } action

Web Element Manager Path

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

firewall policy

This command enables/disables Stateful Firewall support for all subscribers using the current rulebase. In 8.0, this configuration was present in the Subscriber/APN mode.

CLI (Rulebase Configuration Mode)

firewall policy firewall-required

{ default | no } firewall policy

Web Element Manager Path

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

firewall port-scan

This command configures port-scan detection parameters.

CLI (ACS Configuration Mode)

firewall port-scan { connection-attempt-success-percentage { non-scanner | scanner } *percentage* **| inactivity-timeout** *inactivity_timeout* **| protocol { tcp | udp } response-timeout** *response_timeout* **| scanner-policy { block inactivity-timeout** *inactivity_timeout* **| log-only } }**

default firewall port-scan { connection-attempt-success- percentage { non-scanner | scanner } | inactivity-timeout | protocol { tcp | udp } response-timeout | scanner-policy }

Web Element Manager Path

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

firewall priority

This command adds and specifies the priority and type of a firewall rule definition in the rulebase, and allows you to configure a single or range of ports to be allowed on the server for auxiliary/data connections.

CLI (Rulebase Configuration Mode)

firewall priority *priority* **[dynamic-only | static-and-dynamic] firewall-ruledef** *ruledef_name* **{ { permit [trigger open-port {** *aux_port_number* **| range** *start_port_number* **to** *end_port_number* **} direction { both | reverse | same }] } | { deny [charging-action** *charging_action* **] } }**

no firewall priority *priority*

Web Element Manager Path

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

firewall tcp-first-packet-non-syn

This command configures the action to take on TCP flow starting with a non-syn packet.

CLI (Rulebase 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.

firewall tcp-idle-timeout-action

This command configures the action to take on TCP idle timeout expiry.

CLI (Rulebase Configuration Mode)

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

Web Element Manager Path

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

firewall track-list

This command configures the maximum number of server IPs to be tracked that are involved in any kind of DOS attacks.

CLI (ACS Configuration Mode)

`firewall track-list attacking-servers` *`no_of_servers`*
`default firewall track-list attacking-servers`

Web Element Manager Path

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

flow any-error

This command configures the accounting action for packets dropped by Firewall due to any error.

CLI (Rulebase Configuration Mode)

`flow any-error charging-action` *`charging_action`*
`default flow any-error`

Web Element Manager Path

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

nat policy

This command enables/disables Network Address Translation (NAT) processing for all subscribers using this rulebase.

CLI (Rulebase Configuration Mode)

```
nat policy nat-required
{ default | no } nat policy
```

Web Element Manager Path

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

Firewall Commands - New in Release 8.3

IMPORTANT

The new commands documented in this section are only available in Release 8.3.

firewall tcp-reset-message-threshold

This command configures a threshold on the number of TCP reset messages sent by the subscriber for a particular data flow. After this threshold is reached, further downlink traffic to the subscriber on the unwanted flow is blocked.

CLI (Rulebase Configuration Mode)

`firewall tcp-reset-message-threshold` *`messages`* **`then-block-server`**

`{ default | no } firewall tcp-reset-message-threshold`

Web Element Manager Path

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

GGSN Commands - New in Release 8.0

This section provides information on new commands available in Release 8.0.

bearer-control-mode

This new command configures the bearer control mode for network controlled QoS (NCQoS) feature.

CLI (APN Configuration Mode)

bearer-control-mode [ms-only | mixed]

[default] bearer-control-mode

Web Element Manager Path

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

gtpu udp-checksum insert

Use this command to enable the system to insert UDP checksum in outgoing UDP data packets.

CLI (GGSN Service Configuration Mode)

gtpu udp-checksum insert

default gtpu udp-checksum insert

Web Element Manager Path

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

nai-construction

Added new command in APN configuration mode to configure NAI construction for user authentication in GPRS/UMTS networks.

CLI (APN Configuration Mode)

nai-construction {imsi | msisdn} [override-null-username]

default nai-construction

Web Element Manager Path

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

qos negotiate-limit

This new command configures the traffic shaping and policing related parameters.

CLI (APN Configuration Mode)

qos negotiate-limit direction { downlink | uplink } [class { background | conversational | interactive *traffic_priority* **| streaming }] [peak-data-rate** *bps* **[committed-data-rate** *bps* **] | committed-data-rate [peak-data-rate** *bps* **]]**

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

Web Element Manager Path

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

qos rate-limit

This new command configures the traffic shaping and policing related parameters.

CLI (APN Configuration Mode)

qos rate-limit { downlink | uplink } [class { background | conversational | interactive *traffic_priority* **| streaming }] [burst-size** *bytes* **] [exceed-action { drop | lower-ip-precedence | transmit }[violate-action { drop | lower-ip-precedence | shape [transmit-when-buffer-full] | transmit }]][violate-action { drop | lower-ip-precedence | shape [transmit-when-buffer-full] | transmit } [exceed-action { drop | lower-ip-precedence | transmit }]] +**

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

Web Element Manager Path

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

GGSN Commands - New in Release 8.1

The following commands are new to the GGSN in Release 8.1:

clear gtpp storage-server local file statistics

This command clears the statistics for CDRs stored on the local SMC hard disk.

CLI (Exec Mode)

clear gtpp storage-server local file statistics [group name *name***]**

credit-control-group

This command configures the Credit Control Group to be used for subscribers configured for a particular APN.

CLI (APN Configuration Mode)

credit-control-group *cc_group_name*

no credit-control-group

Web Element Manager Path

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

gtpp compression-process

This command configures the maximum number of child compression processes that AAAproxy can have. This functionality is a part of the hard disk support processes.

CLI (Global Configuration Mode)

gtpp compression-process *max_number*

default gtpp compression-process

Web Element Manager Path

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

gtpp dead-server suppress-cdrs

New command added to configure the action to be taken on the CDRs generated during communication failure between GGSN and GTPP servers. It also disables the archive of CDRs.

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.

gtpp ram-disk-limit

This command configures additional storage space to be allocated for writing files. The memory specified with this command would be added to the existing memory allocated to the AAAproxy only if hard disk storage is enabled.

CLI (Global Configuration Mode)

gtpp ram-disk-limit mb *mega_bytes*
default gtpp ram-disk-limit

Web Element Manager Path

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

gtpp secondary-group

New command added to enable/associate a preconfigured secondary GTPP server group to an APN for CGF accounting functionality. By default it is disabled.

CLI (APN Configuration Mode)

gtpp secondary-group *group_name* **[accounting-context** *actt_ctxt_name***]**
[no | default] gtpp secondary-group *group_name*

Web Element Manager Path

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

gtpp storage-server local file

This command configures the parameters for the GTPP files to be stored on the local GTPP storage server. Support for 'custom6' has been added to provide 8K block structure for billing CDR files

CLI (GTPP Group Configuration Mode)

gtpp storage-server local file { compression { gzip | none } | format { custom1 | custom2 | custom3 | custom4 | custom5 | custom6 } | name prefix *prefix* **| rotation { cdr-count** *count* **| time-interval** *time* **| volume** *size* **} }**
default gtpp storage-server local file { compression | format | name | rotation }
no gtpp storage-server local file rotation { cdr-count | time-interval }

Web Element Manager Path

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

gtpp storage-server mode

This command specifies where CDRs will be stored -- on an external server of on a hard disk on the SMC in the ST40 chassis.

CLI (GTPP Group Configuration Mode)

gtpp storage-server mode { local | remote }
default gtpp storage-server mode

Web Element Manager Path

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

gtpp storage-server mode

New keyword “streaming” added to support backup for streaming CDRs on a hard disk on the SMC in the ST40 chassis.

CLI (GTPP Group Configuration Mode)

```
gtpp storage-server mode { local | remote | streaming }
default gtpp storage-server mode
```

Web Element Manager Path

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

IMPORTANT

This is a customer-specific feature.

gtpp suppress-cdrs zero-volume-and-duration

This command suppresses the CDRs created by session having zero duration and/or zero volume. By default this mode is ‘disabled’

CLI (GTPP Group Configuration Mode)

```
gtpp suppress-cdrs zero-volume-and-duration { gcdrs [egcdrs] | egcdrs
[gcdrs] }
default gtpp suppress-cdrs zero-volume-and-duration
```

Web Element Manager Path

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

gtpp transport-layer

New command added to provide facility to select the transport layer protocol for Ga interface between AGWs (GSNs) and GTPP servers. By default selected transport layer protocol is UDP.

CLI (GTPP Group Configuration Mode)

```
gtpp transport-layer { tcp | udp }
default gtpp transport-layer
```

Web Element Manager Path

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

GGSN Commands - New in Release 8.3

This section provides information on new commands available in Release 8.3.

hd raid

Added requirement to confirm commands.

CLI (HD RAID Configuration Mode)

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

```
overwrite { invalid | unknown | valid } disk
[ -noconfirm ]
```

Web Element Manager Path

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

HA Commands - New in Release 8.0

This section provides information on new commands available in Release 8.0.

wimax-3gpp2 interworking

New command added in HA Configuration mode to configure the interworking between 3GPP2 and WiMAX technology networks.

CLI (HA Configuration Mode)

```
[no | default] wimax-3gpp2 interworking
```

Web Element Manager Path

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

HA Commands - New in Release 8.1

This section provides information on new commands available in Release 8.1.

delay interval

Configure the delay time, for starting the dead timer, after configuration files are loaded.

CLI (SRP Configuration Mode)

`hello-interval`

Web Element Manager Path

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

PDIF Commands - New in Release 8.0

PDIF is not supported in Release 8.0.

PDIF Commands - New in Release 8.1

certificate

Apply an X.509 certificate to a crypto template, or remove it, or include or preclude the certificate in the Auth Exchange response payload

CLI (Crypto Template Config Mode

[no | default] certificate *name* **include-payload**

Web Element Manager Path

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

certificate

Create or negate an X.509 trusted certificate.

CLI (Context Config Mode)

[no] certificate name *name* **pem { data** *cert_data* **| url** *cert_url* **}**
private-key pem { [encrypted] data *private_key_data* **| url** *url* **}**

Web Element Manager Path

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

diameter authentication failure-handling

This command configures error handling for Diameter EAP requests.

CLI (AAA Server Group Configuration & Context Configuration Modes)

[no] diameter authentication failure-handling { eap-request |
eap-termination-request } { request-timeout action { continue | terminate }
} | result-code *result_code* **[to** *result_code* **] action { continue |**
retry-and-terminate | terminate } }

Web Element Manager Path

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

diameter disable endpoint

This command disables a diameter peer without removing the peer's configuration.

CLI (Exec Mode)

diameter disable endpoint *endpoint_name* **peer** *peer_id*

Web Element Manager Path

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

diameter enable endpoint

This command enables a diameter peer that is disabled.

CLI (Exec Mode)

diameter enable endpoint *endpoint_name* **peer** *peer_id*

Web Element Manager Path

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

duplicate-session-detection

Configured in the PDIF-Service mode, **`duplicate-session-detection`** configures the PDIF to check for any attempt to set up a call after a MS comes back into WiFi range using either the IMSI or NAI address from a call lost after the MS initially went out of WiFi AP range. Detection can be based on either the IMSI or NAI (default) address. If NAI is used, it must be the NAI from Stage One authentication.

CLI (PDIF-Service Config Mode)

`duplicate-session-detection {` *`NAI`* **`|`** *`IMSI`* **`}`**

Web Element Manager Path

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

group

Diffie-Hellman Group 14 has been added to the existing Groups 1, 2 and 5 for IKEv2 security exchanges.

CLI (IKEv2 Security Association Configuration Mode

`group { 1 | 2 | 5 | 14 }`

Web Element Manager Path

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

ignore-rekeying-requests

Configured in the Crypto Template Payload Config Mode, this is a new command that prevents the creation of a CHILD SA.

CLI (Crypto Template Payload Config Mode)

`ignore-rekeying-requests`

Web Element Manager Path

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

ikev2-ikesa

Configured in the Crypto Template Config Mode, the keyword **`rekey`** has been added to **`ikev2-ikesa`** commands. It specifies if IKESA rekeying should occur before the configured lifetime expires (at approximately 90% of the lifetime interval). Default is **`no ikev2-ikesa rekey.`**

CLI (Crypto Template Config Mode)

`[ no ] ikev2-ikesa [ rekey ]`

Web Element Manager Path

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

ip source-violation

Source validation requires the source address of received packets to match the IP address assigned to the subscriber. IP source-violation sets parameters for allowing bad packets before terminating the call.

CLI (PDIF-Service Config Mode)

ip source-violation { clear-on-valid-packet | drop-limit *num* **| period** *secs* **}**

no ip source-violation clear-on-valid-packet

Web Element Manager Path

Configuration | PDIF Service | Configuration

ipv6 address

Enable this ipv6 address when the Service Redundancy Protocol determines this chassis to be active for Session Recovery .

CLI (loopback-interface-config-mode)

ipv6 address *2001:268:2008:b::1021/128* **srp-activate**

Web Element Manager Path

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

nai

Configures the NAI parameters to be used for the crypto template IDr. This configured IDr is sent from PDIF to MS in the first IKEv2 AUTH response. The default configuration is **no nai**. As a result, the default behavior is for the PDIF-service IP address to be sent as the IDr value with the type ID_IP_ADDR.

CLI (Crypto-Template Config Mode)

[default | no] nai idr *name* **id-type { rfc822-addr | fqdn | ip-addr | key-id }**

Web Element Manager Path

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

radius accounting pdif trigger-policy

Configures the policy for dealing with packet overflow.

CLI (AAA Group Config Mode)

r**adius accounting pdif trigger-policy {** *counter-rollover* | *standard* **}**

Web Element Manager Path

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

rekey

Configured in the Crypto Template Payload Config Mode, the keyword **keepalive** has been added to the **rekey** command. If **keepalive** is configured, a session will be rekeyed even if there has been no data exchanged since the last rekeying operation. By default, rekeying is only performed if there has been data exchanged since the previous rekey.

CLI (Crypto Template Payload Config Mode)

[no] rekey [keepalive]

Web Element Manager Path

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

tsi start-address

Configures the IKEv2 Initiator Traffic Selector (TSI) payload address options.

CLI (Crypto Template Payload Mode)

tsi start-address { any { end-address *any* **} | endpoint { end-address** *endpoint* **} }**

Web Element Manager Path

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

PDSN Commands - New in Release 8.0

This section provides information on new commands available in Release 8.0.

clear credit-control statistics

This command clears the credit-control statistics.

CLI (Exec Mode)

clear credit-control statistics cc-service <*name*>

Web Element Manager Path

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

ipv6 router advertisement

New command added in Ethernet Interface Configuration mode to enables or disables the system to send IPv6 router advertisements.

CLI (Ethernet Interface Configuration Mode)

[no] ipv6 router advertisement

Web Element Manager Path

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

mobile-ipv6

This new command configures Mobile IPv6 related parameters for a subscriber.

CLI (Subscriber Configuration Mode)

[default | no] mobile-ipv6 { home-address *ipv6_address* **| home-agent** *ipv6_address* **| home-link-prefix** *ipv6_address* **| tunnel mtu** *value* **}**

Web Element Manager Path

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

qos traffic-shape

This new command configures the traffic shaping related parameters.

CLI (Subscriber Configuration Mode)

qos traffic-shape direction { downlink | uplink } [burst-size *bytes* **] [committed-data-rate** *bps* **] [exceed-action { drop | lower-ip-precedence | transmit }] [peak-data-rate** *bps* **] [violate-action { drop | lower-ip-precedence | buffer [transmit-when-buffer-full] | transmit }] +**

no qos traffic-shape direction { downlink | uplink }

Web Element Manager Path

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

policy ipv6 tunnel

Tunnel MTU for IPv6 Tunnel between HA and Mobile Node.

CLI (Subscriber Config Mode)

`policy ipv6 tunnel mtu exceed { fragment | notify-sender }`

`mtu exceed { fragment | notify-sender }`

Web Element Manager Path

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

PDSN Commands - New in Release 8.1

This section provides information on new commands available in Release 8.1.

accounting trigger

This command configures an accounting trigger policy map to selectively start and terminate accounting sessions based on the categorization of traffic as being interesting or non-interesting to support the QCHAT Billing Suppression feature.

CLI (Traffic Policy-Map Configuration Mode)

```
[ no ] accounting trigger { inactivity-timeout stop | interesting-traffic start }
```

Web Element Manager Path

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

ip routing overlap-pool

This command provides the ability to advertise overlap-pool addresses into routing

CLI (config-context mode)

```
[ no | default ] ip routing overlap-pool
```

Web Element Manager Path

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

Session Control Manager Commands - New in Release 8.0

Session Control Manager is not supported in Release 8.0.

Session Control Manager Commands - New in Release 8.1

This section provides information on new commands available in Release 8.1.

authorization

This command configures the policy to allow early bandwidth authorization. Default is disabled.

CLI (CSCF Policy Rules Configuration Mode)

[default | no] authorization early-bandwidth

Web Element Manager Path

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

interface

This command enables the collection of interface SIP statistics in a CSCF service.

CLI (CSCF Service Configuration Mode)

[no] interface statistics sip

Web Element Manager Path

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

nat-policy

This command configures a NAT (Network Address Translation) policy for the service if the CSCF service is performing one of the following functions:

- CSCF services are run in bridging (Back-to-Back User Agent) mode
- A-BG is an Application-level Gateway (ALG) for NAT

CLI (CSCF Service Configuration Mode)

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

no nat-policy *policy_name*

Web Element Manager Path

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

plmn-id

This command configures the MCC+MNC pair (plmn-id) used to match location specific emergency/service numbers. Default is disabled.

CLI (CSCF Proxy-CSCF Configuration Mode)

plmn-id mcc *code* **mnc** *code*

no plmn-id

Web Element Manager Path

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

policy

This command configures the overload response for this policy. When the P-CSCF/A-BG becomes congested, this overload policy is used to reject subsequent sessions or redirect them to another server.

CLI (CSCF Policy Rules Configuration Mode)

```
policy overload { redirect address1 [ weight weight1 ]
[ address2 [ weight weight2 ] ] ...
| reject [ use-reject-code { admin-prohibited | insufficient-resources } ]}
default policy overload
no policy overload redirect address1 [ address2 ] ...
```

Web Element Manager Path

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

policy

This command configures the policy for Served User Routing in this S-CSCF service.

CLI (CSCF Serving-CSCF Configuration Mode)

```
[ default | no ] policy allow p-served-user-routing
```

Web Element Manager Path

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

sip-header

This command enables SIP P-Access-Network-Info (PANI) or P-User-Database (PUD) header insertion for the P-CSCF/A-BG service.

CLI (CSCF Proxy-CSCF Configuration Mode)

```
[ no ] sip-header insert { p-access-network-info | p-user-database }
```

Web Element Manager Path

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

sip-param

This command enables the addition of “integrity-protected” parameter in the authorization header of a SIP (REGISTER) message for the P-CSCF/A-BG service.

CLI (CSCF Proxy-CSCF Configuration Mode)

```
[ no ] sip-param insert integrity-protected
```

Web Element Manager Path

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

SGSN Commands - New in Release 8.0

This section provides information on new commands available in Release 8.0.

accept-procedure

This keyword enables the use of either a new TLLI (temporary logical link identifier) or an old TLLI for attach-accept or RAU-accept messages sent by the SGSN to the MS during related procedures. Default is **new-tlli.**

CLI (GPRS Service config mode)

gmm accept-procedure [new-tlli | old-tlli]

Web Element Manager Path

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

accounting

The new accounting command in the GPRS Service configuration mode enables the configuration of the type of CDRs to be generated and also defines the context in which the CDRs are generated.

CLI (GPRS Service Configuration Mode)

accounting (cdr-types *type* **| context** *ctxt_name* **}**

Web Element Manager Path

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

accounting

The new command associates an accounting context and optionally a previously defined GTPP group with an SGSN operator policy.

CLI (SGSN Operator Policy Configuration Mode)

accounting context ctxt_name [gtpp group grp_name]

Web Element Manager Path

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

associate-service

This new command specifies which Gs, MAP, and/or SGTP services are to be associated with a GPRS service.

CLI (GPRS Service Configuration Mode)

[no] associate-service { gs *name* **| map** *name* **| sgtp** *name* **} [context** *ctxt_name* **]**

Web Element Manager Path

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

bssgp-timer

The command configures BSS GP timer parameters in Network Service Entity-Frame Relay or IP configuration mode in a 2.5G GPRS frame relay or IP network connection.

CLI (Network Service Entity Frame Relay Configuration Mode and Network Service Entity - IP Configuration Mode)

bssgp-timer { T2 *time* **| Th** *time* **}**

Web Element Manager Path

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

ciphering-algorithm

This command defines the usage order (priority) for GPRS encryption algorithms for ciphering.

CLI (GPRS Service Configuration Mode)

ciphering-algorithm priority *priority algorithm*

default ciphering-algorithm priority *priority*

Web Element Manager Path

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

gmm information-in-messages

This command is added to provide the configuration to include the information in messages for the GPRS mobility management (GMM) parameters.

CLI (SGSN Operator Policy Configuration Mode)

gmm information-in-messages access-type {{gprs |umts } [network-name {full-text name | short-text name } | [send-after { attach | rau }] }

[default | no] gmm { information-in-messages access-type { gprs | umts }

Web Element Manager Path

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

gmm retrieve-equipment-identity

This command is added to configure the International Mobile Equipment Identity (IMEI) or software version (SV) retrieval and validation procedure for SGSN operator policy.

CLI (SGSN Operator Policy Configuration Mode)

gmm retrieve-equipment-identity {imei | imeisv [unciphered] [then-imei]} [verify-equipment-identity [deny-greylisted]]

[no | default] gmm retrieve-equipment-identity

Web Element Manager Path

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

gtp send

This command configures which information this operator policy specifies for sending in a GTP message. This command includes the following send options:

- RAT
- ULI
- IMEISV
- MS-timezone

CLI (SGSN Operator Policy Configuration Mode)

[no | remove] gtp send *send_option*

Web Element Manager Path

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

iu-recovery

This command enables the IU recovery function to be used whenever sessions are recovered.

CLI (IuPS Service Configuration Mode)

[no] iu-recovery

Web Element Manager Path

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

llc

This command configures the timers that control the data flow for the logical link control (LLC) sub-layer for the GPRS service.

CLI (GPRS Service Configuration Mode)

llc { T200-sapi1-timeout *time* **| T200-sapi11-timeout** *time* **| T200-sapi3-timeout** *time* **| T200-sapi5-timeout** *time* **| T200-sapi7-timeout** *time* **| T200-sapi9-timeout** *time* **} +**

Web Element Manager Path

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

mtp2-lssu-len

This command sets the length of the link status signal unit (LSSU) which carries link status information used to manage link alignment and indicate the status of the signaling points to each other.

CLI (Link Configuration Mode)

mtp2-lssu-len *#_octets*

default mtp2-lssu-len

Web Element Manager Path

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

network-initiated-pdp-activation

This command configures the Operator Policy to support activation of network-initiated PDP contexts and defines any desired activation restrictions.

CLI (SGSN Operator Policy Configuration Mode)

network-initiated-pdp-activation {allow | primary | restrict | secondary} +

Web Element Manager Path

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

network-overload-protection

This new command enables an attach rate throttle mechanism to configure the number of attaches per second and to specific the action to be taken if the limit is exceeded.

CLI (Global Configuration Mode)

network-overload-protection sgsn-new-connections-per-second *#_attaches*
action { drop | reject with cause { congestion | network failure } }
default network-overload-protection sgsn-new-connections-per-second

Web Element Manager Path

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

peer-network-service-entity

The command creates a Peer Network Service Entity instance in the Network Service Entity IP configuration mode to define the peer network service entity.

CLI (Network Service Entity IP Configuration Mode)

[no] peer-network-service-entity name *name*

Web Element Manager Path

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

pool

This command enables the default SGSN functionality for SGSN (flex) pooling and enables inclusion of the configured count for pool hop-counter in new SGSN context/identify request messages.

CLI (SGTP Service Configuration Mode)

pool { default-sgsn | hop-counter count }
default pool hop-counter
no pool { default-sgsn | hop-counter }

Web Element Manager Path

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

rab-modify-procedure

This command configures how the RAB (radio access bearer) assignment procedure will be modified

CLI (RNC Config Mode)

```
rab-modify-procedure { normal-modify | release-and-establish }
default rab-modify-procedure
```

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 (Radio Network Controller 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.

re-authenticate

Enables or disables the re-authentication feature.

CLI (RNC Config Mode)

```
re-authenticate [ access-type { gprs | umts }
remove re-authenticate
```

Web Element Manager Path

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

release-compliance

Configures data rate management per RNC by defining the 3GPP release compliance (R6 or R7) of the RNC.

CLI (RNC Config Mode)

```
release-compliance { pre-release-7 | release-7 }
default release-compliance
```

Web Element Manager Path

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

relocation-complete-timeout

Specifies the maximum time to wait for a relocation completion in the core network.

CLI (IuPS Service Config Mode)

relocation-complete-timeout timeout_value
default relocation-complete-timeout

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.

resolver

This command configures, or resets to default, either of the two parameters for the DNS resolver function: the number of retries or the retransmission timer.

CLI (DNS Client Configuration Mode)

[default] resolver {number-of-retries *retries* **| retransmission-interval** *time***}**

Web Element Manager Path

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

retries

The command configures the number of retries for different events in a virtual connection in the Network Service Virtual Connection configuration mode.

CLI (Network Service Virtual connection Configuration Mode)

retries { ns-alive-retry *num_retries* **| ns-block-retry** *num_retries* **| ns-reset-retry** *num_retries* **| ns-unblock-retry** *num_retries* **}**

Web Element Manager Path

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

retry-count

The command configures the retry-count parameters for NS-alive and SNS procedures in the Network Service Entity IP configuration mode.

CLI (Network Service Entity IP Configuration Mode)

retry-count { ns-alive *max* **| sns-proc** *max* **}**

Web Element Manager Path

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

sctp-max-out-strms

This command sets the maximum number of outbound streams for a specific PSP.

CLI PSP Configuration Mode)

sctp-max-out-strms *max#_out_streams*
default sctp-max-out-strms

Web Element Manager Path

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

sctp-suppress-alarm

This new command is added to enable/disable the suppression of alarms for SCTP path failure between two peer endpoints.

CLI (PSP Configuration Mode)

[no] sctp-suppress-alarm path-failure self-end-point-address *orig_ipv4_address* **peer-end-point-address** *peer_ipv4_address*

Web Element Manager Path

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

setup-timeout

This new command sets the maximum number of seconds allowed for session setup.

CLI (GPRS Service Configuration Mode)

[default] setup-timout *seconds*

Web Element Manager Path

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

sgsn-context-request

This new command tells the system to perform or to skip the PTMSI signature check if the PTMSI signature is not included in the SGSN context request.

CLI (GPRS Service Configuration Mode)

[default] sgsn-context-request ptmsi-signature-absence allowed

Web Element Manager Path

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

sgsn offload

This command sets or stops the off loading of subscribers, which is part of the SGSN's Gb flex load redistribution functionality.

CLI (Exec Mode)

sgsn offload gprs-service *srvc_name* **{ activating | connecting } [nri-value | stop | t3312-timeout** *seconds***]**

Web Element Manager Path

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

sgsn imsimgr

This command manages the IMSI auditing performed by the IMSIMgr in combination with one or more SessMgr(s).

CLI (Exec Mode)

sgsn imsimgr { add-record *imsi* sessmgr instance *sessmgr#* | audit-with sessmgr { all | instance *sessmgr#* } | remove-record *imsi* }

Web Element Manager Path

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

short-message-service

This command enables or disables the SGSN's SMS service as well as providing access to the SMS Service Configuration Mode and the commands to fine-tune the SMS operation.

CLI (MAP Service Configuration Mode)

short-message-service

Web Element Manager Path

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

sm

This command configures the SM layer parameter associated with this particular GPRS service context.

CLI (GPRS Service Configuration Mode)

sm { activate-max-retransmissions *num_retries* **| deactivate-max-retransmissions** *num_retries* **| modify-max-retransmissions** *num_retries* **| t3385-timeout** *secs* **| t3386-timeout** *secs* **| t3395-timeout** *secs* **}**

default sm { activate-max-retransmissions | deactivate-max-retransmissions | modify-max-retransmissions | t3385-timeout | t3386-timeout | t3395-timeout }

Web Element Manager Path

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

sm

The **requested-apn-from-first subrec** keyword enables the selection of an APN from the first subscription record as APN(R). If this feature is enabled, the PDP Activation is not rejected during APN Selection; instead, the APN from the first subscription record is used as the requested APN and the SGSN continues with the rest of the APN Selection process.

CLI (GPRS Service Configuration Mode)

sm requested-apn-from-first-subrec

Web Element Manager Path

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

threshold per-service-gprs-pdp-sessions

The command configures the thresholds for the total number of PDP contexts for the GPRS sessions per GPRS service.

CLI (Global Configuration Mode)

threshold per-service-grps-pdp-sessions *high_thresh* **[clear** *low_thresh* **]**

Web Element Manager Path

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

threshold per-service-gprs-sessions

The command configures the thresholds for the GPRS sessions per GPRS service.

CLI (Global Configuration Mode)

threshold per-service-grps-sessions *high_thresh* **[clear** *low_thresh* **]**

Web Element Manager Path

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

threshold poll per-service-gprs-pdp-sessions interval

The command configures the polling interval during which thresholds are measured.

CLI (Global Configuration Mode)

threshold poll per-service-gprs-pdp-sessions interval *time*

Web Element Manager Path

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

threshold poll total-gprs-pdp-sessions interval

The command configures the polling interval during which thresholds are measured.

CLI (Global Configuration Mode)

threshold poll total-gprs-pdp-sessions interval *time*

Web Element Manager Path

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

threshold poll per-service-gprs-sessions interval

The command configures the polling interval during which thresholds are measured.

CLI (Global Configuration Mode)

threshold poll per-service-gprs-sessions interval *time*

Web Element Manager Path

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

threshold poll total-gprs-sessions interval

The command configures the polling interval during which thresholds are measured.

CLI (Global Configuration Mode)

threshold poll total-gprs-sessions interval *time*

Web Element Manager Path

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

threshold total-gprs-pdp-sessions

The command configures the thresholds for the total number of PDP contexts for the GPRS sessions in the system.

CLI (Global Configuration Mode)

threshold total-gprs-pdp-sessions *high_thresh* **[clear** *low_thresh* **]**

Web Element Manager Path

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

threshold total-gprs-sessions

The command configures the thresholds for the total number of GPRS sessions in the system.

CLI (Global Configuration Mode)

threshold total-gprs-sessions *high_thresh* **[clear** *low_thresh* **]**

Web Element Manager Path

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

timeout

The command configures the timeout parameter for different events in a virtual connection in the Network Service Virtual Connection configuration mode.

CLI (Network Service Virtual Connection Configuration Mode)

timer { ns-alive-timeout *duration* **| ns-block-timeout** *duration* **|**
ns-reset-timeout *duration* **| ns-test-timeout** *duration* **}**

Web Element Manager Path

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

timer

The command configures the timers for SNS-Prov and TNS-Test in the Network Service Entity IP configuration mode.

CLI (Network Service Entity IP Configuration Mode)

timer { SNS-Prov-Timeout *time* **| TNS-Test-Timeout** *time***}**

Web Element Manager Path

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

vlan-map

This command configures a single IPv4 or IPv6 address multiple vlans to use for a single next-hop gateway.

CLI (Ethernet Interface Configuration Mode and VLAN Configuration Mode)

vlan-map next-hop *ip_address*

Web Element Manager Path

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

weight

This command configures the signaling and data weight for the network service virtual link (NSVL) for the NSE-IP end-point.

CLI (NSVL Configuration Mode)

weight { data *data_weight* **| signaling** *signaling_weight* **}**

Web Element Manager Path

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

SGSN Commands - New in Release 8.1

The following commands are new to the SGSN in Release 8.1:

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.

check-imei-timeout-action

This command configures the action to be taken on the Gf interface if a Check-IMEI fails due to a timeout.

CLI (SGSN or GPRS Service Configuration Modes)

check-imei-timeout-action [continue | reject]

default check-imei-timeout-action

Web Element Manager Path

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

clear gtpp storage-server local file statistics

This command clears the statistics for CDRs stored on the local SMC hard disk.

CLI (Exec Mode)

```
clear gtpp storage-server local file statistics [ group name name ]
```

clock-source

This command sets the source of the port's transmit clock.

CLI (Port Channelized Configuration Mode)

```
clock-source { internal-timing | loop-timing }
```

Web Element Manager Path

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

dns israu-mcc-mnc-encoding

This command configures either decimal or hexadecimal format for the MCC and MNC values in the DNS query.

CLI (GRPS Service Configuration Mode)

CLI (SGSN Service Configuration Mode)

dns israu-mcc-mnc-encoding { decimal | hexidecimal }
default dns israu-mcc-mnc-encoding

Web Element Manager Path

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

gtpp compression-process

This command configures the maximum number of child compression processes that AAAproxy can have. This functionality is a part of the hard disk support processes.

CLI (Global Configuration Mode)

gtpp compression-process *max_number*
default gtpp compression-process

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.

gtpp ram-disk-limit

This command configures additional storage space to be allocated for writing files. The memory specified with this command would be added to the existing memory allocated to the AAAproxy only if hard disk storage is enabled.

CLI (Global Configuration Mode)

gtpp ram-disk-limit mb *mega_bytes*
default gtpp ram-disk-limit

Web Element Manager Path

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

gtpp storage-server local file

This command configures the parameters for the GTPP files to be stored on the local GTPP storage server. Support for ‘custom6’ has been added to provide 8K block structure for billing CDR files.

CLI (GTPP Group Configuration Mode)

gtpp storage-server local file { compression { gzip | none } | format { custom1 | custom2 | custom3 | custom4 | custom5 | custom6} | name prefix *prefix* **| rotation { cdr-count** *count* **| time-interval** *time* **| volume** *size* **} }**

default gtpp storage-server local file { compression | format | name | rotation }

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

Web Element Manager Path

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

gtpp storage-server mode

This command specifies where CDRs will be stored -- on an external server of on a hard disk on the SMC in the ST40 chassis.

CLI (GTPP Group Configuration Mode)

gtpp storage-server mode { local | remote }

default gtpp storage-server mode

Web Element Manager Path

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

gtpp suppress-cdrs zero-volume-and-duration

This command suppresses the CDRs created by sessions having zero duration and/or zero volume. By default this mode is ‘disabled’

CLI (GTPP Group Configuration Mode)

gtpp suppress-cdrs zero-volume-and-duration { gcdrs [egcdrs] | egcdrs [gcdrs] }

default gtpp suppress-cdrs zero-volume-and-duration

Web Element Manager Path

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

gtpp transport-layer

A new keyword has been added to configure either UDP or TCP as the Ga interface transport layer between SGSN and GTPP servers. By default, UPD protocol is enabled for transport layer.

CLI (GTPP Group Configuration Mode)

gtpp transport-layer { tcp | udp }

default gtpp transport-layer

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.

link-type

This keyword is not yet functional - the feature is still in development. This keyword will only be applicable to releases 8.1 and higher.

Identifies the signalling type for this link.

CLI (SGSN Linkset Configuration Mode)

link id *id* [link-type [atm-broadband | highspeed-narrowband | lowspeed-narrowband]

Web Element Manager Path

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

network-sharing cs-ps-coordination

This command enables/disables the SGSN service to perform a CS-PS coordination check.

CLI (SGSN Service Configuration Mode)

network-sharing cs-ps-coordination

default network-sharing cs-ps-coordination

no network-sharing cs-ps-coordination

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.

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.

routing-context

This command sets the routing context instructions included in the M3UA messages.

CLI (SGSN PSP Configuration Mode)

```
routing-context { discard-inbound | process-inbound } { insert-outbound |
suppress-outbound }
```

Web Element Manager Path

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

sgsn-number

This command defines the SGSN's E.164 number to associate with the Gs Service.

CLI (Gs Service Configuration Mode)

sgsn-number <E.164_number>

Web Element Manager Path

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

super-charger

This command enables/disables the SGSN to work with a super-charged network.

CLI (SGSN Operator Policy Configuration Mode)

```
super-charger
remove super-charger
```

Web Element Manager Path

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

Modified Configuration Commands

Common Commands - Modified in Release 8.0

This section provides information on commands modified for Release 8.0.

cca quota-state

This command specifies the quota state of a subscriber for prepaid credit control service. The **lower-bandwidth** keyword was added to this command. When configured, this state matches the lower-bandwidth quota state of a rating group.

CLI (Ruledef Configuration Mode)

[no] cca quota-state *operator* **{ limit-reached | lower-bandwidth }**

Web Element Manager Path

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

clear subscriber sgsn-service

New sgsn-service keyword clears all PDP contexts associated with a specific SGSN service. This keyword can be used with filtering keywords that are part of the clear subscriber command set. Using this command can trigger a network-initiated service request (paging) procedure.

CLI (Exec Mode)

clear subscriber sgsn-service name [filter_keyword]

Web Element Manager Path

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

clock

Added following new time zones to this command:

- newzealand-auckland (GMT +12:00; Auckland, Wellington)
- newzealand-chatham (GMT +12:45; Chatham)

CLI (Global Configuration Mode)

clock timezone *tz* **[local]**
no clock timezone

Web Element Manager Path

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

congestion-control policy

The following congestion-control policies were added:

- **mipv6ha-service**
- **pdif-service**
- **sgsn-service**

CLI (Global Configuration Mode)

congestion-control policy {asngw-service | asnpc-service | cscf-service | ggsn-service | ha-service | lns-service | mipv6ha-service | pdif-service | pdsn-service | sgsn-service } action
{ drop | none | redirect | reject }

Web Element Manager Path

Click Monitoring | Congestion Control to view the **pdif-service** congestion control policy. The other policies are not supported at this time.

diameter accounting

The **dictionary** keyword was added to the **diameter accounting** command.

CLI (AAA Server Group and Context Configuration Mode)

diameter accounting { dictionary { aaa-custom1 | aaa-custom10 | aaa-custom2 | aaa-custom3 | aaa-custom4 | aaa-custom5 | aaa-custom6 | aaa-custom7 | aaa-custom8 | aaa-custom9 | nasreq | rf-plus } | endpoint *endpoint_name* **| max-retries** *tries* **| max-transmissions** *transmissions* **| request-timeout** *duration* **| server** *host_name* **priority** *priority* **}**

[no] diameter accounting { endpoint | max-retries | max-transmissions | server *host_name* **}**

[default] diameter accounting { dictionary | max-retries | max-transmissions | request-timeout }

Web Element Manager Path

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

diameter authentication

The **dictionary** keyword was added to the **diameter authentication** command.

CLI (AAA Server Group and Context Configuration Modes)

diameter authentication { dictionary { aaa-custom1 | aaa-custom10 | aaa-custom2 | aaa-custom3 | aaa-custom4 | aaa-custom5 | aaa-custom6 | aaa-custom7 | aaa-custom8 | aaa-custom9 | nasreq } | endpoint *endpoint_name* **| max-retries** *tries* **| max-transmissions** *transmissions* **| request-timeout** *duration* **| server** *host_name* **priority** *priority* **}**

[no] diameter authentication { endpoint | max-retries | max-transmissions | server *host_name* **}**

[default] diameter authentication { dictionary | max-retries | max-transmissions | request-timeout }

Web Element Manager Path

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

diameter pending-timeout

The **after-expiry-try-secondary-host** keyword was removed from the **diameter pending-timeout** command. This feature can now be managed using the **retry-after-tx-expiry** and **go-offline-after-tx-expiry** keywords available in the **failure-handling** command.

CLI (Credit Control Configuration Mode)

diameter pending-timeout *duration*

default diameter pending-timeout

Web Element Manager Path

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

failure-handling

The following keywords were added to this command:

- **initial-request**
- **terminate-request**
- **update-request**
- **retry-after-tx-expiry**
- **go-offline-after-tx-expiry**

CLI (Credit Control Configuration Mode)

failure-handling { initial-request | terminate-request | update-request } { continue [go-offline-after-tx-expiry | retry-after-tx-expiry] | retry-and-terminate [retry-after-tx-expiry] | terminate }

default failure-handling [initial-request | terminate-request | update-request]

Web Element Manager Path

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

failure-handling

This command configures the failure handling behavior for flow or protocol in Enhanced-Policy Decision Function (E-PDF). The **any-error** keyword was added to this command. This enables configuring failure handling behavior for those result-codes for which failure-handling behavior has not been specified.

CLI (Policy Control Configuration Mode)

failure-handling { continue | retry-and-terminate | terminate | diameter-result-code { any-error | integer *result_code* **} ccfh { continue | retry-and-terminate | terminate } [cc-request-type { initial-request | terminate-request | update-request }] }**

no failure-handling diameter-result-code { any-error | integer *result_code* **} [cc-request-type { initial-request | terminate-request | update-request }]**

Web Element Manager Path

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

file

This command configures EDR file parameters. The following changes have been made to this command:

- The **file-sequence-number rulebase-seq-num** keyword was added to the command. This keyword enables generating file sequence numbers on a per rulebase basis with the rulebase name and format name.
- The **num-records** option was added to the **file rotation** keyword. This option enables limiting the file size by number of records.
- On ST40 chassis, the maximum amount of space available for storage of EDR/UDR files configured using the **storage-limit** keyword has changed.

  On ST40 chassis, the total storage limit is 536870912 bytes (512 MB). On ST16 chassis, the total storage limit is 268435456 bytes (256 MB). This limit is for UDR and EDR files combined.

CLI (EDR Module Configuration Mode)

file [charging-service-name { include | omit }] [compression { gzip | none }] [current-prefix *string* **] [delete-timeout** *seconds* **] [directory** *dir_name* **] [edr-format-name] [exclude-checksum-record] [field-separator { hyphen | omit | underscore }] [file-sequence-number rulebase-seq-num] [headers] [name** *file_name* **] [reset-indicator] [rotation [num-records** *number* **| time** *seconds* **| volume** *bytes* **]] [sequence-number { omit | padded | padded-six-length | unpadded }] [storage-limit** *limit* **] [time-stamp { expanded-format | rotated-format | unix-format }] [trailing-text** *string* **] [trap-on-file-delete] [xor-final-record] +**

default file [charging-service-name] [compression] [current-prefix] [delete-timeout] [directory] [edr-format-name] [field-separator] [file-sequence-number] [headers] [name] [reset-indicator] [rotation { num-records | time | volume }] [sequence-number] [storage-limit] [time-stamp] [trailing-text] +

Web Element Manager Path

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

file

This command configures UDR file parameters. The following changes were made to this command:

- The **file-sequence-number rulebase-seq-num** keyword was added to the command. This keyword enables generating file sequence numbers on a per rulebase basis with the rulebase name and format name.
- The **num-records** option was added to the **file rotation** keyword. This option enables limiting the file size by number of records.
- On ST40 chassis, the maximum amount of space available for storage of EDR/UDR files configured using the **storage-limit** keyword has changed.

  On ST40 chassis, the total storage limit is 536870912 bytes (512 MB). On ST16 chassis, the total storage limit is 268435456 bytes (256 MB). This limit is for UDR and EDR files combined.

CLI (UDR Module Configuration Mode)

file [charging-service-name { include | omit }] [compression { gzip | none }] [current-prefix *string* **] [delete-timeout** *seconds* **] [directory** *dir_name* **] [exclude-checksum-record] [field-separator { hyphen | omit | underscore }] [file-sequence-number rulebase-seq-num] [headers] [name** *file_name* **] [reset-indicator] [rotation [num-records** *number* **| time** *seconds* **| volume** *bytes* **]] [sequence-number { omit | padded | padded-six-length | unpadded }] [storage-limit** *limit* **] [time-stamp { expanded-format | rotated-format | unix-format }] [trailing-text** *string* **] [trap-on-file-delete] [udr-seq-num] [xor-final-record] +**

default file [charging-service-name] [compression] [current-prefix] [delete-timeout] [directory] [field-separator] [file-sequence-number] [headers] [name] [reset-indicator] [rotation { num-records | time | volume }] [sequence-number] [storage-limit] [time-stamp] [trailing-text] [udr-seq-num]

Web Element Manager Path

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

frame-relay

This command defines the Frame Relay characteristics of the port - the word ‘channel’ was removed from the command.

CLI (Channelized Port Configuration Mode)

frame-relay path *path_id* **{ ds1** *connects* **| e1** *connects***} [timeslots | frame-relay [intf-type** *intf_type* **[lmi_type** *lmi_type* **]]]**

Web Element Manager Path

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

lawful-intercept

Added new keyword **all** for this command to use with **no** keyword to clear all warrant information in one single command **no lawful-intercept all**:

CLI (Exec Mode)

no lawful-intercept [all] { [imei *imei_value*] **[imsi** *imsi_value* **] [ip-addr** *intercept_ip_addr* **] [msid** *ms_id* **] [msisdn** *msisdn_value*] **[username** *subscriber_name* **] + } [calltype** *call_type* **]**

Web Element Manager Path

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

logging filter runtime facility

Additional facility options have been added to the **logging filter** command in the Global Configuration Mode. Those with an * (asterisk) are for the SGSN.

- *bssap+: Bssap+ logging facility
- *bssgp: BSSGP Protocol logging facility
- *cap: CAP Protocol logging facility
- chatconf: Voice Chat/Conference logging facility

- credit-control: Credit Control facility
- demuxmgr: Demux Manager API facility
- dgmbmgr: Diameter Gmb Application Manager logging facility
- dhcpv6: DHCPV6
- ds3mgr: DS3 Manager logging facility
- eap-ipsec: EAP
- ecs-css: ACSMGR <-> Session Manager Signalling Interface Logging facility
- * gmm: GMM Protocol logging facility
- * gprs-ns: GPRS-NS Protocol logging facility
- hdctrl: HD Controller logging facility
- igmp: IGMP
- ikev2: IKEv2
- ims-sh: HSS SH Service facility
- imsimgr: SGSN IMSI Manager facility
- ipsg: IP Service Gateway interface logging facility
- kvstore: KV Store facility
- * linkmgr: SGSN/SS7 Links Manager facility
- * llc: LLC Protocol logging facility
- * m3ua: M3UA Protocol logging facility
- * map: MAP Protocol logging facility
- megadiammgr: Megadiameter Manager (SLF Service)
- mmgr: Master Manager logging facility
- mobile-ipv6: Mobile IPv6 control logging facility
- * mtp3: MTP3 Protocol logging facility
- pdif: PDIF logging facility
- pmm-app: PMM application logging facility
- ptt: Voice push-to-talk logging facility
- push: VPNMGR CDR push logging facility
- * ranap: RANAP Protocol logging facility
- * sccp: SCCP Protocol logging facility
- * sctp: SCTP Protocol logging facility
- * sgsn-app: SGSN-APP interface logging facility
- * sgsn-gtpc: SGSNs GTP-C Protocol logging facility
- * sgsn-gtpu: SGSNs GTP-U Protocol logging facility
- * sgsn-misc: SGSN miscellaneous logging facility
- * sgsn-system: SGSNs System Components logging facility
- * sgsn-test: SGSN Tests logging facility
- * sgtpcmgr: SGSN GTPC Manager facility

- * sm-app: SM Protocol logging facility
- * sms: SMS Service logging facility
- * sndcp: SNDCP Protocol logging facility
- * sscfnni: SSCFNNI Protocol logging facility
- * sscop: SSCOP Protocol logging facility
- * taclcp: TAC Local Call Processing logging facility
- * tcap: TCAP Protocol logging facility
- ttg: TTG logging facility
- tucl: TUCL logging facility
- vim: Voice Instant Messaging logging facility
- vinfo: Voice Information logging facility
- vmgctrl: Virtual Media Gateway Controller logging facility
- vmgctxmgr: VMG Context Manager logging facility

newcall policy

The **mipv6ha-service** keyword was added to the syntax.

CLI (Exec Mode)

newcall policy mipv6ha-service { all | name service_name } reject

Web Element Manager Path

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

ping

The **broadcast** keyword was added to the syntax.

CLI (Exec Mode)

ping hostname broadcast

Web Element Manager Path

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

bind

Added new license-enabled keywords to configure traffic from the specified DHCP service bind address to use the MPLS labels. This support also provides the configuration to define nexthop gateway address:

CLI (DHCP Service Configuration Mode)

bind address *ip_address* **[nexthop-forwarding-address** *nexthop_ip_address*
[mpls-label input *in_mpls_label_value* **output** *out_mpls_label_value1*
[*out_mpls_label_value2* **]]]**

no bind address *ip_address*

Web Element Manager Path

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

Common Commands - Modified in Release 8.1

IMPORTANT

The commands documented in this section are only available in Release 8.1.

accounting trigger

New option “default” is added and the “start” and “stop” stop keywords have been deprecated (removed).

CLI (Traffic Policy-Map Configuration Mode Commands)

[no | default] accounting trigger { inactivity-timeout | interesting-traffic | intra-service-handoff }

Web Element Manager Path

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

attribute

This command specifies the order of fields to appear within an EDR. The following attributes were added to this command:

- sn-parent-protocol: Parent protocol of flow.
- sn-subscriber-nat-flow-ip: NAT IP address of NAT-enabled subscriber.
- sn-subscriber-nat-flow-port: NAT port number of NAT-enabled subscriber.

CLI (EDR Format Configuration Mode)

attribute *attribute* **{ [format { MM/DD/YY-HH:MM:SS | MM/DD/YYYY-HH:MM:SS | YYYY/MM/DD-HH:MM:SS | YYYYMMDDHHMMSS | seconds }] [localtime] | [{ ip | tcp } { bytes | pkts } { downlink | uplink }] priority** *priority* **}**

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

Web Element Manager Path

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

attribute

This command specifies the order of fields to appear within an UDR. The following attribute was added to this command:

- sn-subscriber-nat-flow-ip: NAT IP address of NAT-enabled subscriber.

CLI (UDR Format Configuration Mode)

attribute *attribute* **{ [format { MM/DD/YY-HH:MM:SS | MM/DD/YYYY-HH:MM:SS | YYYY/MM/DD-HH:MM:SS | YYYYMMDDHHMMSS | seconds } [localtime] | [{ bytes | pkts } { downlink | uplink }]] priority** *priority* **}**

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

Web Element Manager Path

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

bcmcs

This command has been modified by adding the optional keyword **encrypted** so the password *grppasswd* can be sent either encrypted or clear.

CLI (PDSN-Service Config Mode)

[encrypted] grppasswd *group_passwd*

Web Element Manager Path

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

cdr

This command configures the CDR file transfer parameters. The **transfer-mode** keyword was enhanced to support EDR/UDR push via SPIO. Previously, the push was support only via LC.

CLI (EDR Module Configuration Mode & UDR Module Configuration Mode)

cdr [[push-interval *value* **] [remove-file-after-transfer] [transfer-mode { pull | push primary { encrypted-url** *enc_url* **| url** *url* **} [via local-context] [secondary { encrypted-secondary-url** *enc_sec_url* **| url** *sec_url* **}] }] + | use-harddisk]**

no cdr [remove-file-after-transfer | use harddisk] +

default cdr [push-interval | remove-file-after-transfer | transfer-mode [push via] | use harddisk] +

Web Element Manager Path

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

clear crypto

This command has been modified to clear all IKEv2 statistics for the current context, or to clear statistics based on service ip address or service name.

CLI (Exec Mode)

clear crypto statistics { ikev2 [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.

framing

The ability to identify the path-type (either E1 or DS1/T1) has been added to the **framing** command for use with the CLC2 SONET or SDH configuration.

CLI (Channelized Port Configuration Mode)

framing { ethernet | sdh [ds1 | e1] | sonet [ds1 | e1] | unspecified } [-noconfirm]

Web Element Manager Path

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

iiop port

The **no** keyword has been added to the iiop port command.

CLI (ORBEM Config mode)

no iiop port

Web Element Manager Path

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

ip access-list

This command enables creating/configuring/deleting an IP Access List in the current context. The access list name to be specified has been restricted to be an alpha and/or numeric string of 1 through 47 characters in length. In StarOS 8.0, it can be an alpha and/or numeric string of 1 through 79 characters in length.

CLI (Context Configuration Mode)

ip access-list *name*

[default | no] ip access-list *name*

Web Element Manager Path

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

ip pool

The **nat-realm** keyword was added to this command. This enables to designate an IP address pool as a Firewall Network Address Translation (NAT) realm pool.

CLI (Context Configuration Mode)

ip pool *name* **{** *ip_address subnet_mask* **|** *ip_addr_mask_combo* **| range** *start_address end_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* **] [nat-realm users-per-nat-ip-address** *users* **[on-demand [address-hold-timer** *address_hold_timer* **]]] [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]**

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] [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.

mobile-ip send

This command includes two new options for the **send** keyword:

- accounting-correlation-info
- imsi

CLI (Subscriber Config Mode)

[no] mobile-ip send { accounting-correlation-info | dns-address | imsi | terminal-verification }

Web Element Manager Path

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

port-switch-on-l3-fail

This command has been extended to support ipv6 addresses

CLI (Ethernet Interface Config Mode)

port-switch-on-L3-fail address { *ip_address* **|** *ipv6_address* **}**

Web Element Manager Path

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

radius accounting max-outstanding

The maximum number of outstanding messages a single AAA manager instance will queue has been set to 4000.

CLI (AAA Group Config Mode & Context Config Mode)

radius accounting max-outstanding *msgs*

Web Element Manager Path

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

radius charging accounting server

The maximum number of outstanding messages that may be allowed to the server has been set to 4000.

CLI (AAA Group Config Mode & Context Config Mode)

radius charging accounting server *ip_address* **[encrypted] key** *string* **max** *msgs*

Web Element Manager Path

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

radius charging max-outstanding

The maximum number of outstanding messages a single AAA manager instance will queue has been set to 4000.

CLI (AAA Group Config Mode & Context Config Mode)

radius charging max-outstanding *msgs*

Web Element Manager Path

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

radius charging server

The maximum number of outstanding messages that may be allowed to the server has been set to 4000.

CLI (AAA Group Config Mode & Context Config Mode)

radius charging server *ip_address* **[encrypted] key** *string* **max** *msgs*

Web Element Manager Path

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

radius max-outstanding

The maximum number of outstanding messages a single AAA manager instance will queue has been set to 4000.

CLI (AAA Group Config Mode & Context Config Mode)

radius max-outstanding *msgs*

Web Element Manager Path

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

radius server

The maximum number of outstanding messages that may be allowed to the server has been set to 4000.

CLI (AAA Group Config Mode & Context Config Mode)

radius server *ip_address* **[encrypted] key** *string* **max** *msgs*

Web Element Manager Path

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

service-type

This command configures the type of service (Frame Relay or pwe3-cse) to be employed on the CLC or CLC2 (channelized line cards).

CLI (Card Configuration Mode)

service-type { frame-relay | pwe3-cesopsn | unspecified }
default service-type

Web Element Manager Path

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

show srp

New option “call-loss statistics” is added to show history of calls lost during switchover.

CLI (Excec Mode Commands)

```
show srp { call-loss statistics | checkpoint statistics
[verbose ] | info | statistics } | [ grep grep_options | more
]
```

Web Element Manager Path

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

Common Commands - Modified in Release 8.3

IMPORTANT

This section provides information on commands modified in Release 8.3.

attribute

This command specifies the order of fields to appear within an EDR. The following attributes were added to this command:

- sn-nat-binding-timer: Port chunk hold timer.
- sn-nat-gmt-offset: GMT offset of the node generating NAT bind record.
- sn-nat-ip: NAT IP address of the port chunk.
- sn-nat-last-activity-time-gmt: The time when the last flow in a specific NAT set of flows was seen.
- sn-nat-port-block-end: Last port number of the port chunk.
- sn-nat-port-block-start: Starting port number of the port chunk.
- sn-nat-port-chunk-alloc-dealloc-flag: Indicates whether the port chunk is allocated or released.
- sn-nat-port-chunk-alloc-time-gmt: Indicates when the port chunk was allocated.
- sn-nat-port-chunk-dealloc-time-gmt: Indicates when the port chunk was released.
- sn-nat-realm-name: Name of the NAT realm.
- sn-nat-subscribers-per-ip-address: Subscriber(s) per NAT IP address.

CLI (EDR Format Configuration Mode)

attribute *attribute* **{ [format { MM/DD/YY-HH:MM:SS | MM/DD/YYYY-HH:MM:SS | YYYY/MM/DD-HH:MM:SS | YYYYMMDDHHMMSS | seconds }] [localtime] | [{ ip | tcp } { bytes | pkts } { downlink | uplink }] priority** *priority* **}**

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

Web Element Manager Path

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

ip pool

This command enables adding, updating, or deleting an IP address pool in the current context. The following keywords and several options were added to this command:

- **nat-one-to-one**: This keyword enables configuring one-to-one NAT realm pool.
- **napt-users-per-ip-address**: This keyword enables configuring the number of users sharing a single NAT IP address for a many-to-one NAT realm.

The following keyword was removed from this command:

- **nat-realm**

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.

readdress server commands in inbound IPv4 ACLs

Prior to Release 8.3, for packets received from the packet data network destined for a subscriber's UE, the system applied logic to reset the source address of a packet to the original destination address of the input packet before applying the outbound ACL (access control list). In Release 8.3 and higher, the system reverses the order and applies the outbound ACL before resetting the source address. This change impacts all current readdress server rules in inbound IPv4 ACLs.

After upgrading to Release 8.3, for every readdress server rule in an inbound IPv4 ACL, customers must now add a permit rule to an outbound ACL that explicitly permits packets from the readdress rule's redirect address and port number. If customers omit this permit rule, the system will reject all packets destined for the subscriber's UE from the readdress rule's redirect address and port number.

deny/permit (by TCP/UDP packets)

This command was modified to include the range option for PDIF Release 8.3.

CLI (Access Control List Configuration Mode)

permit { tcp | udp } [range *start_port end_port* **]**

Web Element Manager Path

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

threshold cpu-orbs-warn

The default is changed for this command. The default is now 50.

CLI (Global Config Mode Commands)

threshold cpu-orbs-warn *high_thresh* **[clear** *low_thresh* **]**

Web Element Manager Path

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

threshold cpu-orbs-crit

The default is changed for this command. The default is now 60.

CLI (Global Config Mode Commands)

threshold cpu-orbs-crit *high_thresh* **[clear** *low_thresh* **]**

Web Element Manager Path

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

CF Commands - Modified in Release 8.0

This section provides information on CF commands modified in Release 8.0.

analyze

The *cat_string* variable in **category** keyword in this command is now changed to provide explicit category name to configure analysis priority.

CLI (CFP Configuration Mode)

analyze priority *priority* **{ all | category** *cat_string* **} action { allow | content-insertion** *content_string* | **discard | redirect-url** *url* **| terminate-flow }**

Web Element Manager Path

Click Configuration | Active Charging | Active Charging Services

analyze

This command specifies the action to take for the indicated result after content filtering analysis. An optional keyword "**edr** *edr_format_name*" was added to this command for EDR generation based on content category and action.

CLI (CFP Configuration Mode)

analyze priority *priority* **{ all | category** *cat_string* **} action { allow | content-insertion** *content_string* | **discard | redirect-url** *url* **| terminate-flow } [edr** *edr_format_name***]**

edr_format_name is the name of a pre-defined EDR file format name in the *EDR Format Configuration Mode*.

Web Element Manager Path

Click Configuration | Active Charging | Active Charging Services

CF Commands - Modified in Release 8.1

This section provides information on CF commands modified in Release 8.1.

analyze

This command specifies the action to take for the indicated result after content filtering analysis. The following keywords were added to this command:

- **www-reply-code-and-terminate-flow**
- **x-category**

The following category options were added to the **category** keyword:

- **ENERGY**
- **STREAM**
- **VOIP**

The following category options were removed from the **category** keyword:

- **ADV**
- **AUCT**
- **CLEAN**
- **CPORN**
- **P2P**
- **PHISH**
- **RADIO**
- **SFTWRE**
- **SPYWRE**
- **SUSP**

CLI (Content Filtering Policy Configuration Mode)

analyze priority *priority* **{ all | category** *cat_string* **| x-category** *string* **} action { allow | content-insert** *content_string* **| discard | redirect-url** *url* **| terminate-flow | www-reply-code-and-terminate-flow** *reply_code* **} [edr** *edr_format_name* **]**

no analyze priority *priority*

Web Element Manager Path

Click Configuration | Active Charging | Active Charging Services

content-filtering

This command enables/disables the Category Policy Identifier for Content Filtering support, and enters the Content Filtering Policy Configuration Mode. The description option allows the operator to provide a description for the CF Category Policy ID. Both the *description* keyword and the argument *desc_string* are now optional. This enables adding and removing the descriptions.

CLI (ACS Configuration Mode)

content-filtering category policy-id *cf_policy_id* **[description [** *desc_string* **]] [-noconfirm]**

no content-filtering category policy-id *cf_policy_id*

Web Element Manager Path

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

content-filtering category policy-id

This command configures the Content Filtering Category Policy Identifier for Policy-based Content Filtering support in a rulebase. Now, while removing the configured category policy from the rulebase, optionally the policy ID can be specified. If the specified policy ID is invalid, or is not configured in the rulebase, an error message is displayed. If no policy ID is specified, whatever policy is configured, if any, is removed from the rulebase.

CLI (Rulebase Configuration Mode)

content-filtering category policy-id *cf_policy_id*

no content-filtering category policy-id [*cf_policy_id* **]**

Web Element Manager Path

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

timeout action

This command specifies the actions when the content filtering analysis results are not available to analyze. The **www-reply-code-and-terminate-flow** keyword was added to this command.

CLI (Content Filtering Policy Configuration Mode)

timeout action { allow | content-insert *content_string* **| discard | redirect-url** *url* **| terminate-flow | www-reply-code-and-terminate-flow** *reply_code* **} [edr** *edr_format_name* **]**

default timeout action [edr *edr_format_name* **]**

Web Element Manager Path

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

ECS Commands - Modified in Release 8.0

This section provides information on ECS commands in Release 8.0.

action

This command assigns an action priority to a rule definition. The **group-of-ruledefs** keyword was added to this command. This enables assigning a group of rule definitions to the rulebase.

CLI (Rulebase Configuration Mode)

action priority *action_priority* **{ [dynamic-only | static-and-dynamic] { ruledef** *name* **| group-of-ruledefs** *name* **} charging-action** *name* **[description** *desc* **] }**

no action-priority *action_priority*

Web Element Manager Path

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

bearer imsi

This command defines a rule definition to analyze and charge user traffic using an International Mobile Station Identification number (IMSI) in bearer flow. The **{ !range | range } imsi-pool** *imsi_pool* **}** option was added to this command. This enables the IMSI number to be selected from a range configured in an IMSI pool.

CLI (Ruledef Configuration Mode)

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

Web Element Manager Path

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

charge-volume

This command configures the volume counter for eG-CDR and DCCA charging calculation. The packet-length keyword was added to this command. This enables to configure charge volume for packet length.

CLI (Charging Action Configuration Mode)

charge-volume { *protocol* **{ bytes | packet-length | packets } [downlink | uplink] | constant** *value* **}**

[no | default] charge-volume

Web Element Manager Path

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

charging-rule-optimization

This command configures the amount of internal optimization for improved performance when evaluating each instance of the action CLI command. There is no external change to this command, only that now “www url =” kind of rules under the ambit of charging-rule-optimization in rulebase. Until now, setting “charging-rule-optimization” to “medium” or “high” would only optimize the “starts-with” and “contains” rules, not the “=” rules. Now the “=” rules are also optimized.

CLI (Rulebase Configuration Mode)

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

`default charging-rule-optimization`

Web Element Manager Path

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

dictionary

This command specifies the dictionary to use for requests to the server(s) in a Content Filtering Server Group. The **`custom2`** keyword was added to this command.

CLI (Content Filtering Server Group Configuration Mode)

`dictionary { custom1 | custom2 | standard }`
`[ default | no ] dictionary`

Web Element Manager Path

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

flow action

This command specifies the actions for packets that match a rule definition. The following changes were made to this command:

- The **`discard`** keyword now includes the **`downlink`** and **`uplink`** options. This enables selecting specific packets.
- The **`readdress`** keyword was added to this command. This enables specifying a re-address server for the charging action.

CLI (Charging Action Configuration Mode)

`flow action { conditional user-agent end-token` *`end_token_name`* **`| discard [ downlink | uplink ] | readdress { server`** *`ip_address`* **`[ port`** *`port_number`* **`] | port`** *`port_number`* **`} | redirect-url`** *`url`* **`[ clear-quota-retry-timer ] | terminate-flow }`**

`no flow action`

Web Element Manager Path

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

flow limit-across-applications

The **non-tcp** *limit* and **tcp** *limit* keywords were added to this command. This command can now also be used to limit the total number of flows per Subscriber/APN sent to a rulebase based on the protocol type.

CLI (Rulebase Configuration Mode)

flow limit-across-applications { *limit* **| non-tcp** *limit* **| tcp** *limit* **}**
[no] flow limit-across-applications [non-tcp | tcp]

Web Element Manager Path

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

flow limit-for-bandwidth

This command enables and configures bandwidth limits for Session Control functionality to the subscriber. The **exceed-action** keyword is now optional.

CLI (Charging Action Configuration Mode)

[no | default] flow limit-for-bandwidth direction { downlink | uplink }
peak-data-rate *bps* **peak-burst-size** *bytes* **violate-action { discard |**
lower-ip-precedence } [committed-data-rate *bps* **committed-burst-size** *bytes*
[exceed-action { discard | lower-ip-precedence }]]

Web Element Manager Path

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

ip dst-address

This command defines rule definition to analyze and charge user traffic based on Internet Protocol (IP) destination address. The "**{ !range | range } host-pool** *host_pool*" option was added to this command. This enables the IP destination address to be selected from a range configured in a host pool.

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 server-ip-address

This command defines rule definition to analyze and charge user traffic matching the Internet Protocol (IP) address of the destination, i.e. from the subscriber, of the connection. The **{ !range | range } host-pool** *host_pool* option was added to this command. This enables the IP address to be selected from a range configured in a host pool.

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 rule definition to analyze and charge user traffic based on Internet Protocol (IP) source address. The **{ !range | range } host-pool** *host_pool* option was added to this command. This enables the IP source address to be selected from a range configured in a host pool.

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 rule definition to analyze and charge user traffic matching the Internet Protocol (IP) address of the subscriber (either source address or destination address). The **{ !range | range } host-pool** *host_pool* option was added to this command. This enables the IP address to be selected from a range configured in a host pool.

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.

ip tos

This command sets the IP Type of Service (ToS) octets being used in the charging action. The option to allow the IP TOS to be set using a numeric value was added to this command.

CLI (Charging Action Configuration Mode)

ip tos { *tos_value* **| af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | ef } [uplink | downlink]**

no ip tos [uplink | downlink]

Web Element Manager Path

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

mms bcc

The "**case-sensitive**" keyword was added to this command.

CLI (Ruledef Configuration Mode)

[no] mms bcc [case-sensitive] *operator string*

Web Element Manager Path

Click Configuration | Active Charging | Active Charging Service and click Add or Modify.

mms cc

The "**case-sensitive**" keyword was added to this command.

CLI (Ruledef Configuration Mode)

[no] mms cc [case-sensitive] *operator string*

Web Element Manager Path

Click Configuration | Active Charging | Active Charging Service and click Add or Modify.

mms content location

The "**case-sensitive**" keyword was added to this command.

CLI (Ruledef Configuration Mode)

[no] mms content location[case-sensitive] *operator string*

Web Element Manager Path

Click Configuration | Active Charging | Active Charging Service and click Add or Modify.

mms content type

The "**case-sensitive**" keyword was added to this command.

CLI (Ruledef Configuration Mode)

[no] mms content type [case-sensitive] *operator string*

Web Element Manager Path

Click Configuration | Active Charging | Active Charging Service and click Add or Modify.

mms from

The "**case-sensitive**" keyword was added to this command.

CLI (Ruledef Configuration Mode)

[no] mms from [case-sensitive] *operator string*

Web Element Manager Path

Click Configuration | Active Charging | Active Charging Service and click Add or Modify.

mms message-id

The "**case-sensitive**" keyword was added to this command.

CLI (Ruledef Configuration Mode)

[no] mms message-id [case-sensitive] *operator string*

Web Element Manager Path

Click Configuration | Active Charging | Active Charging Service and click **Add** or **Modify**.

mms subject

The "**case-sensitive**" keyword was added to this command.

CLI (Ruledef Configuration Mode)

[no] mms subject [case-sensitive] *operator string*

Web Element Manager Path

Click Configuration | Active Charging | Active Charging Service and click **Add** or **Modify**.

mms to

The "**case-sensitive**" keyword was added to this command.

CLI (Ruledef Configuration Mode)

[no] mms to [case-sensitive] *operator string*

Web Element Manager Path

Click Configuration | Active Charging | Active Charging Service and click Add or Modify.

p2p protocol

This command configures the system to detect specific P2P protocols for charging purposes. The following P2P protocol options have been added to this command:

- applejuice
- ares
- directconnect
- feidian
- filetopia
- gadugadu
- imesh
- manolito
- mute
- pando
- pplive
- ppstream
- qq
- qqlive

- skinny
- sopcast
- soulseek
- zatoo

CLI (Ruledef Configuration Mode)

```
[ no ] p2p protocol = { applejuice | ares | bittorrent | directconnect |
edonkey | fasttrack | feidian | filetopia | gadugadu | gnutella | imesh |
jabber | manolito | msn | mute | orb | pando | pplive | ppstream | qq |
qqlive | skinny | skype | slingbox | sopcast | soulseek | winny | 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 specific peer-to-peer (P2P) protocols. The following P2P protocol options have been added to this command:

- applejuice
- ares
- directconnect
- feidian
- filetopia
- gadugadu
- imesh
- manolito
- mute
- pando
- pplive
- ppstream
- qq
- qqlive
- skinny
- sopcast
- soulseek
- zatoo

CLI (Active Charging Configuration Mode)

```
[ no ] p2p-detection protocol [ all | applejuice | ares | bittorrent |
directconnect | edonkey | fasttrack | feidian | filetopia | gadugadu |
gnutella | imesh | jabber | manolito | msn | mute | orb | pando | pplive |
ppstream | qq | qqlive | skinny | skype | slingbox | sopcast | soulseek |
winny | yahoo | zattoo ]+
```

Web Element Manager Path

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

ruledef

This command creates a rule definition for the Active Charging Service, and enters ACS Ruledef Configuration Mode. The "**description** *string*" keyword was removed from this command.

CLI (ACS Configuration Mode)

[no] ruledef *ruledef_name* **[-noconfirm]**

Web Element Manager Path

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

rule-variable

This command configures the event rule variable for EDR file format attribute. The following rules were added to this command:

- http protocol: user-agent
- bearer protocol: ggsn-address

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.

tcp either-port

This command defines rule definition to analyze and charge user traffic using either (destination or source) TCP port. The **{ !range | range } port-map** *port_map* option was added to this command. This enables the port number to be selected from a range configured in a port map.

CLI (Ruledef Configuration Mode)

[no] tcp either-port { *operator port_number* **| { !range | range } {** *start_range* **to** *end_range* **| port-map** *port_map* **} }**

Web Element Manager Path

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

tcp dst-port

This command defines rule definition to analyze and charge user traffic based on destination Transmission Control Protocol (TCP) port. The **{ !range | range } port-map** *port_map* option was added to this command. This enables the port number to be selected from a range configured in a port map.

CLI (Ruledef Configuration Mode)

[no] tcp dst-port { *operator port_number* **| { !range | range } {** *start_range* **to** *end_range* **| port-map** *port_map* **} }**

Web Element Manager Path

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

tcp src-port

This command defines rule definition to analyze and charge user traffic based on source Transmission Control Protocol (TCP) port. The **{ !range | range } port-map** *port_map* option was added to this command. This enables the port number to be selected from a range configured in a port map.

CLI (Ruledef Configuration Mode)

[no] tcp src-port { *operator port_number* **| { !range | range } {** *start_range* **to** *end_range* **| port-map** *port_map* **} }**

Web Element Manager Path

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

udp dst-port

This command defines rule definition to analyze and charge user traffic based on destination User Datagram Protocol (UDP) port number. The **{ !range | range } port-map** *port_map* option was added to this command. This enables the port number to be selected from a range configured in a port map.

CLI (Ruledef Configuration Mode)

[no] udp dst-port { *operator port_number* **| { !range | range } {** *start_range* **to** *end_range* **| port-map** *port_map* **} }**

Web Element Manager Path

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

udp either-port

This command defines rule definition to analyze and charge user traffic using either (destination or source) User Datagram Protocol (UDP) port. The **{ !range | range } port-map** *port_map* option was added to this command. This enables the port number to be selected from a range configured in a port map.

CLI (Ruledef Configuration Mode)

[no] udp either-port { *operator port_number* **| { !range | range } {** *start_range* **to** *end_range* **| port-map** *port_map* **} }**

Web Element Manager Path

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

udp src-port

This command defines rule definition to analyze and charge user traffic based on source User Datagram Protocol (UDP) port number. The **{ !range | range } port-map** *port_map* option was added to this command. This enables the port number to be selected from a range configured in a port map.

CLI (Ruledef Configuration Mode)

[no] udp src-port { *operator port_number* **| { !range | range } {** *start_range* **to** *end_range* **| port-map** *port_map* **} }**

Web Element Manager Path

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

license

Configures the session license key.

CLI (Global Configuration Mode Commands)

license key *key_value* [-force] session-limit

no license key *key_value* [-force] session-limit

Web Element Manager Path

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

ECS Commands - Modified in Release 8.1

IMPORTANT

The commands documented in this section have all been modified for Release 8.1.

action priority

This command configures the action priority for a ruledef/group-of-ruledefs in the rulebase. The following keywords were added to this command:

- **timedef** *timedef_name*: Associates the specified time definition with the ruledef/group-of-ruledefs. Timedefs enable activation/deactivation of ruledefs/groups-of-ruledefs such that they are available for rule matching only when they are active.

CLI (Rulebase Configuration Mode)

action priority *action_priority* **{ [dynamic-only | static-and-dynamic | timedef** *timedef_name* **] { group-of-ruledefs** *group_name* **| ruledef** *ruledef_name* **} charging-action** *charging_action_name* **[monitoring-key** *monitoring_key* **] [description** *description* **] }**

no action priority *action_priority*

Web Element Manager Path

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

attribute

This command specifies the order of fields to appear within an EDR. The following new attributes were added to this command:

- transaction-downlink-bytes
- transaction-downlink-packets
- transaction-uplink-bytes
- transaction-uplink-packets

Also, a new closure reason for EDRs has been added: “ACS_EDR_TRANSACTION_COMPLETE_EVENT”. So “attribute sn-closure-reason” in EDRs will populate value 12 (corresponding to closure-reason “ACS_EDR_TRANSACTION_COMPLETE_EVENT”) in EDRs.

CLI (Rulebase Configuration Mode)

attribute *attribute* **{ [format { MM/DD/YY-HH:MM:SS | MM/DD/YYYY-HH:MM:SS | YYYY/MM/DD-HH:MM:SS | YYYYMMDDHHMMSS | seconds }] [localtime] | [{ ip | tcp } { bytes | pkts } { downlink | uplink }] priority** *priority* **}**

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

Web Element Manager Path

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

credit-control

This command enables/disables Prepaid Credit Control Configuration mode. The group keyword was added to this command. This enables configuring credit control groups. This enables applying different credit control configurations (DCCA dictionary, failure-handling, session-failover, Diameter endpoint selection, etc.) to different subscribers on the same system.

CLI (Active Charging Configuration Mode)

[no] credit-control [group *group_name* **]**

Web Element Manager Path

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

flow action

This command specifies the actions for packets that match a rule definition. The **terminate-session** keyword was added to this command. This enables specifying the flow action to terminate session. When a rule pointing to a charging action configured with the terminate-session keyword is hit, then the corresponding session will be terminated.

CLI (Charging Action Configuration Mode)

flow action { conditional user-agent end-token *end_token_name* **| discard [downlink | uplink] | readdress { server** *ip_address* **[port** *port_number* **] | port** *port_number* **} | redirect-url** *url* **[clear-quota-retry-timer] | terminate-flow | terminate-session }**

no flow action

Web Element Manager Path

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

flow action redirect-url

This command specifies the redirection of URL for packets that matches a rule definition. This command also specifies the redirect-URL action on packet and flow for Session Control functionality. This CLI can now be used to redirect SIP requests as well.

CLI (Charging Action Configuration Mode)

flow action redirect-url *url***/%3furl=***dynamic_field* **[clear-quota-retry-timer]**

{ default | no } flow action redirect-url

Web Element Manager Path

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

flow limit-for-bandwidth

This command enables and configures bandwidth limits for Session Control functionality to the subscriber. Uplink and downlink limits are configured separately. The **id** keyword was added to this command. This enables configuring identifier for bandwidth limiting.

CLI (Charging Action Configuration Mode)

flow limit-for-bandwidth { { direction { downlink | uplink } peak-data-rate *bps* **peak-burst-size** *bytes* **violate-action { discard | lower-ip-precedence } [committed-data-rate** *bps* **committed-burst-size** *bytes* **[exceed-action { discard | lower-ip-precedence }]] } | { id** *id* **} }**

{ default | no } flow limit-for-bandwidth { direction { downlink | uplink } | id }

Web Element Manager Path

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

icap server

This command adds an Internet Content Adaptation Protocol (ICAP) server configuration to a Content Filtering Server Group. The **priority** keyword was added to this command. This enables specifying the priority of an ICAP server in a Content Filtering Server Group.

IMPORTANT

The maximum outstanding request per ICAP connection configured using the optional **max** <*max_msgs*> keyword is limited to one. Therefore, other values configured using the **max** keyword will be ignored.

CLI (Content Filtering Server Group Configuration Mode)

icap server *ip_address* **[port** *port_number* **] [max** *msgs* **] [priority** *priority* **]**

no icap server *ip_address* **[port** *port_number* **] [priority** *priority* **]**

Web Element Manager Path

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

insert

This command configures the x-header fields to be inserted in HTTP GET and POST request packets.

The following keywords were added to this command:

- **customer-id**
- **charging-characteristics**
- **imei**

The following keywords were moved from under "**insert** *xheader_field_name* **variable bearer**" to under "**insert** *xheader_field_name* **variable bearer 3gpp**":

- **imsi**
- **sgsn-address**

CLI (x-header Format Configuration Mode)

insert *xheader_field_name* **{ string-constant** *xheader_field_value* **| variable { bearer { 3gpp { charging-characteristics | charging-id | imei | imsi | sgsn-address } | customer-id | ggsn-address | radius-calling-station-id | sn-rulebase | subscriber-ip-address } | http { host | url } }**

no insert *xheader_field_name*

Web Element Manager Path

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

ip protocol

This command defines a rule definition to analyze user traffic based on the protocol being transported by IP packets. The following keywords were added to this command:

- *protocol*: Enables specifying a protocol by its name.
- *operator protocol_assignment*: Enables specifying a protocol lesser than or equal to, or greater than or equal to a protocol assignment number.

CLI (Ruledef Configuration Mode)

[no] ip protocol { { *operator* **{** *protocol* **|** *protocol_assignment* **} } | {** *operator protocol_assignment* **} }**

Web Element Manager Path

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

ip tos

This command sets the IP Type of Service (ToS) octets being used in the charging action. The keyword to set IP ToS using a numeric value was modified to **lower-bits** *tos_value*.

CLI (Charging Action Configuration Mode)

ip tos { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | ef | lower-bits *tos_value* **} [uplink | downlink]**

no ip tos [uplink | downlink]

Web Element Manager Path

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

ping6

This command configures IPv6 ping options. A new keyword **interface** *name* has been added that specifies the originating source interface name.

CLI (Exec Mode Commands)

ping6 interface *name*

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 P2P protocol options have been added to this command in Release 8.1:

- ddlink
- halflife2
- hamachivpn
- irc
- oscar
- popo
- steam
- tvants
- tvuplayer
- uusee
- vpnx
- vtun
- winmx
- wofwarcraft
- xbox

CLI (Ruledef Configuration Mode)

```
[ no ] p2p protocol = { applejuice | ares | bittorrent | ddlink |
directconnect | edonkey | fasttrack | feidian | filetopia | gadugadu |
gnutella | halflife2 | hamachivpn | imesh | irc | jabber | manolito | msn |
mute | 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 specific peer-to-peer (P2P) protocols. The following P2P protocol options have been added to this command in Release 8.1:

- ddlink
- halflife2
- hamachivpn
- irc
- oscar
- popo
- steam
- tvants
- tvuplayer

- uusee
- vpnx
- vtun
- winmx
- wofwarcraft
- xbox

CLI (Active Charging Configuration Mode)

```
[ no ] p2p-detection protocol [ all | applejuice | ares | bittorrent |
ddlink | directconnect | edonkey | fasttrack | feidian | filetopia |
gadugadu | gnutella | halflife2 | hamachivpn | imesh | irc | jabber |
manolito | msn | mute | 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.

require active-charging

This command enables/disables Enhanced Charging Service with or without Category-based Content Filtering application. The following changes were made to this command:

- The **`optimized-mode`** keyword was added to this command. This enables ECS in Optimized mode, wherein enhanced charging facilities run as part of the SessMgr.

IMPORTANT

In Release 8.1, Enhanced Charging Service must be enabled in Optimized mode.

IMPORTANT

By default, on installing Release 8.1, the system comes up with ECS in non-optimized mode. To change to the optimized mode, the **`require active-charging optimized-mode`** command must be saved to the configuration from the CLI, and the system rebooted for the change to take effect.

If the enhanced-charging mode is changed from the default (non-optimized) mode to the Optimized mode, or vice-versa, the system must be rebooted for the change to take effect.

- The **`isolated-mode`** keyword was removed from this command. This keyword is still supported on Release 8.0 and earlier, wherein it enables ECS, and separates ECS-related resources from other sub-system resource sharing.

CLI (Global Configuration Mode)

```
require active-charging [ content-filtering category ] [ optimized-mode ]
no require active-charging
```

Web Element Manager Path

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

rule-variable

This command configures the event rule variable for EDR file format attribute. The following fields were added under “bearer 3gpp” rule:

- imei
- rat-type
- sgsn-address
- user-location-information

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.

ECS Commands - Modified in Release 8.3

IMPORTANT

The commands documented in this section have all been modified for Release 8.3.

file sequence-number

This command configures EDR file parameters. The **length** option was added to the **sequence-number** keyword, this enables to specify the file sequence number length.

CLI (EDR Module Configuration Mode)

file [charging-service-name { include | omit }] [compression { gzip | none }] [current-prefix *string* **] [delete-timeout** *seconds* **] [directory** *dir_name* **] [edr-format-name] [exclude-checksum-record] [field-separator { hyphen | omit | underscore }] [file-sequence-number rulebase-seq-num] [headers] [name** *file_name* **] [reset-indicator] [rotation [num-records** *number* **| time** *seconds* **| volume** *bytes* **]] [sequence-number { length** *length* **| omit | padded | padded-six-length | unpadded }] [storage-limit** *limit* **][time-stamp { expanded-format | rotated-format | unix-format }] [trailing-text** *string* **] [trap-on-file-delete] [xor-final-record] +**

default file [charging-service-name] [compression] [current-prefix] [delete-timeout] [directory] [edr-format-name] [field-separator] [file-sequence-number] [headers] [name] [reset-indicator] [rotation { num-records | time | volume }] [sequence-number] [storage-limit][time-stamp] [trailing-text] +

Web Element Manager Path

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

require active-charging

This command enables/disables Enhanced Charging Service with or without Category-based Content Filtering application. The **optimized-mode** keyword was obsoleted. With or without this keyword ECS is always enabled in Optimized mode.

CLI (Global Configuration Mode)

require active-charging [content-filtering category] [optimized-mode]

no require active-charging

Web Element Manager Path

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

rule-application

This command specifies the application rule for a rule definition. The **post-processing** keyword was added to this command, this enables to specify rule definitions for post-processing purposes.

CLI (Ruledef Configuration Mode)

rule-application { charging | post-processing | routing }

no rule-application

Web Element Manager Path

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

Firewall Commands - Modified in Release 8.0

This section provides information on commands modified for Release 8.0.

firewall policy

This command enables/disables Stateful Firewall support for the subscriber.

CLI (APN Configuration Mode)

`firewall policy firewall-required`
`[ default | no ] firewall policy`

Web Element Manager Path

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

firewall policy

This command enables/disables Stateful Firewall support for the APN.

CLI (Subscriber Configuration Mode)

`firewall policy firewall-required`
`[ default | no ] firewall policy`

Web Element Manager Path

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

Firewall Commands - Modified in Release 8.1

IMPORTANT

The commands documented in this section have been modified in Release 8.1.

firewall dos-protection

This command configures firewall protection from Denial-of-Service (DoS) attacks. In 8.0 this command was available in the Active Charging Service Configuration mode. In 8.1 it was moved to the Rulebase Configuration mode. Also, in 8.1, the **`port-scan`** option was added to this command.

CLI (Rulebase Configuration Mode)

`[ no ] firewall dos-protection { all | flooding { icmp | tcp-syn | udp } | ftp-bounce | ip-unaligned-timestamp | mime-flood | port-scan | seq-number-out-of-range | seq-number-prediction | source-router | teardrop | winnuke }`
`default firewall dos-protection`

Web Element Manager Path

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

firewall flooding

This command configures firewall protection from packet flooding attacks. In 8.0 this command was available in the Active Charging Service Configuration mode. In 8.1 it is moved to the Rulebase Configuration mode.

CLI (Rulebase Configuration Mode)

firewall flooding { { protocol { icmp | tcp-syn | udp } packet limit *packets* **} | { sampling-interval** *interval* **} }**

default firewall flooding { { protocol { icmp | tcp-syn | udp } packet limit } | { sampling-interval } }

Web Element Manager Path

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

firewall icmp-destination-unreachable-message-threshold

This command configures a threshold on the number of ICMP error messages sent by the subscriber for a particular data flow. In 8.0 this command was available in the Active Charging Service Configuration mode. In 8.1 it is moved to the Rulebase Configuration mode.

CLI (Rulebase Configuration Mode)

firewall icmp-destination-unreachable-message-threshold *messages* **then-block-server**

[default | no] firewall icmp-destination-unreachable-message -threshold

Web Element Manager Path

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

firewall max-ip-packet-size

This command configures the maximum IP packet size allowed over firewall. In 8.0 this command was available in the Active Charging Service Configuration mode. In 8.1 it is moved to the Rulebase Configuration mode.

CLI (Rulebase Configuration Mode)

firewall max-ip-packet-size *packet_size* **protocol { icmp | non-icmp }**

default firewall max-ip-packet-size protocol { icmp | non-icmp }

Web Element Manager Path

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

firewall mime-flood

This command configures firewall protection from MIME Flooding attacks. In 8.0 this command was available in the Active Charging Service Configuration mode. In 8.1 it was moved to the Rulebase Configuration mode.

CLI (Rulebase Configuration Mode)

firewall mime-flood { http-headers-limit *max_limit* **|**
max-http-header-field-size *max_size* **}**

default firewall mime-flood { http-headers-limit |
max-http-header-field-size }

Web Element Manager Path

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

firewall no-ruledef-matches

This command configures the default action for packets when no Firewall ruledef matches.

In 8.0 this command was available in the Active Charging Service Configuration mode. In 8.1 it is moved to the Rulebase Configuration mode.

The **nat-realm** keyword was added to this command. This enables to optionally specify a NAT realm to be used for performing NAT on subscriber packets.

CLI (Rulebase Configuration Mode)

firewall no-ruledef-matches { downlink | uplink } action { deny [
charging-action *charging_action* **] | permit [nat-realm** *nat_realm* **] }**

default firewall no-ruledef-matches { downlink | uplink } action

Web Element Manager Path

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

firewall priority

This command adds and specifies the priority and type of a firewall rule definition in the rulebase, and allows to configure a single or range of ports to be allowed on the server for auxiliary/data connections.

The **nat-realm** keyword was added to this command. This enables to optionally specify a NAT realm to be used for performing NAT on subscriber packets matching the firewall ruledef.

CLI (Rulebase Configuration Mode)

firewall priority *priority* **[dynamic-only | static-and-dynamic]**
firewall-ruledef *firewall_ruledef* **{ { deny [charging-action**
charging_action **] } | { permit [nat-realm** *nat_realm* **| trigger open-port {**
aux_port_number **| range** *start_port_number* **to** *end_port_number* **} direction {**
both | reverse | same }] } }

no firewall priority *priority*

Web Element Manager Path

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

firewall tcp-syn-flood-intercept

This command enables and configures the TCP intercept parameters to prevent TCP SYN flooding attacks by intercepting and validating TCP connection requests for DoS protection mechanism configured with the **dos-protection** command. In v8.0 this command was available in the Active Charging Service Configuration mode. In v8.1 it is moved to the Rulebase Configuration mode.

CLI (Rulebase Configuration Mode)

firewall tcp-syn-flood-intercept { max-attempts *max_attempts* **| mode { none | { intercept | watch } [aggressive] } | retransmit-timeout** *retransmit_timeout* **| watch-timeout** *intercept_watch_timeout* **}**

default firewall tcp-syn-flood-intercept { max-attempts | mode | retransmit-timeout | watch-timeout }

Web Element Manager Path

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

ip protocol

This command defines a firewall rule definition to analyze user traffic based on the protocol being transported by IP packets. The following keywords were added to this command:

- *protocol*: Enables specifying a protocol by its name.
- *operator protocol_assignment*: Enables specifying a protocol lesser than or equal to, or greater than or equal to a protocol assignment number.

CLI (Firewall Ruledef Configuration Mode)

[no] ip protocol { { *operator* **{** *protocol* **|** *protocol_assignment* **} } | {** *operator protocol_assignment* **} }**

Web Element Manager Path

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

Firewall Commands - Modified in Release 8.3

IMPORTANT

The commands documented in this section have been modified in Release 8.3.

firewall no-ruledef-matches

This command configures the default action for packets when no Firewall Ruledef matches. The optional keyword **bypass-nat** was added to this command. This enables to configure packets permitted to pass to bypass Network Address Translation (NAT).

CLI (Rulebase Configuration Mode)

firewall no-ruledef-matches { downlink | uplink } action { deny [charging-action *charging_action* **] | permit [bypass-nat | nat-realm** *nat_realm* **] }**

default firewall no-ruledef-matches { downlink | uplink } action

Web Element Manager Path

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

firewall priority

This command adds and specifies the priority and type of a firewall rule definition in the rulebase, and allows to configure a single or range of ports to be allowed on the server for auxiliary/data connections.

The optional keyword **bypass-nat** was added to this command. This enables to configure packets to bypass NAT.

CLI (Rulebase Configuration Mode)

firewall priority *priority* **[dynamic-only | static-and-dynamic] firewall-ruledef** *firewall_ruledef* **{ { deny [charging-action** *charging_action* **] } | { permit [nat-realm** *nat_realm* **| [byass-nat] [trigger open-port {** *aux_port_number* **| range** *start_port_number* **to** *end_port_number* **} direction { both | reverse | same }]] } }**

no firewall priority *priority*

Web Element Manager Path

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

GGSN Commands - Modified in Release 8.0

This section provides information on GGSN commands modified in Release 8.0.

allow aaa-assigned-hostname

Existing command now modified to accommodate new keyword to configure the system to allow different attributes in the LAC Hostname AVP and Called-Number AVP for L2TP messages exchanged between LAC and LNS.

CLI (LAC Service Configuration Mode)

allow {aaa-assigned-hostname | called-number value apn}

[no | defualt] allow {aaa-assigned-hostname | called-number value apn}

Web Element Manager Path

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

bearer-control-mode

New keyword **none** added to exclude the bearer control mode information elements and BCM information in PCO IE in GTP messages in a network where unknown information elements are not ignored by AGWs or firewall results in message drop/reject.

CLI (APN Configuration Mode)

bearer-control-mode [ms-only | mixed | none]

[default] bearer-control-mode

Web Element Manager Path

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

cc profile

This command includes additional tariff timers.

CLI (GGSN Service Configuration Mode)

cc profile *10* **tariff time1** *0 7* **time2** *30 19* **time3** *0 7* **time4** *30 19* **time5** *30 26* **time4** *0 7*

Web Element Manager Path

Click Configuration | GGSN | GGSN Service.

gtpp dictionary

This command designates specific dictionary used by GTPP for specific context. New dictionaries were added to this command.

CLI (Context Configuration and GTPP Server Group Configuration Modes)

gtpp dictionary { custom1 | custom10 | custom11 | custom12 | custom13 | custom14 | custom15 | custom16 | custom17 | custom18 | custom19 | custom2 | custom20 | custom3 | custom4 | custom5 | custom6 | custom7 | custom8 | custom9 | standard }

default gtpp dictionary

Web Element Manager Path

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

gtpp error-response

This command determines whether the GGSN retries sending a DRT request after receiving an error response message.

CLI (GTPP Group Configuration Mode)

gtpp error-response { discard-cdr | retry-request }

default gtpp error-response

Web Element Manager Path

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

gtpp interim now

This command check points current GTPP accounting messages and identifies which types of interim CDRs are to be generated and sent to the external charging/storage servers (e.g., a CFG or a GSS). The impact of this command is immediate. Two new keywords have been added to assist with fine tuning the GTPP messages: **callid** and **dhcp-server**.

CLI (Exec Mode)

gtpp interim now [active-charging egcdr | apn *apn_name* **| callid** *call_id* **| cdr-types { mcdr | scdr } | dhcp-server** *ip_address* **| gprs-service** *svc_name* **| ggsn-service** *svc_name* **| imsi** *imsi* **[ip-address sub_address [username** *name* **] now | nsapi** *nsapi* **[ip-address** *sub-address* **[username** *name* **] | username** *name* **]] | ip-address** *sub_address* **[username** *name* **] | ip-pool** *pool_name* **| mcc** *mcc_number* **mnc** *mnc_number* **| msisdn** *msisdn_num* **| sgsn-address** *ip_address* **| sgsn-service** *svc_name* **| username** *name* **] +**

Web Element Manager Path

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

gtpp max-cdrs

TP PR 4360 ST16 PR 70569

The **default** keyword was added to the syntax.

CLI (GTPP Group Configuration Mode)

[default] gtpp max-cdrs *number* **[wait-time** *seconds* **]**

Web Element Manager Path

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

sgsn-address

New keywords **GAN** and **HSPA** added to support Generic Access Network and High Speed Packet Access type of radio access technology with SGSN address in GGSN service configuration mode.

CLI (GGSN Service Configuration Mode)

sgsn address {{*ip_address* **[subnetmask** *netmask* **]} |**
*ip_address/netmask***}[plmn-foreign [reject-foreign-subscriber]**
| mcc *mcc_code* **mnc** *mnc_code* **[reject-foreign-subscriber]] [rat-type {**
GAN | GERAN | HSPA | UTRAN | WLAN }] [description *description* **]**
[disable-gtpc-echo]

no sgsn { address *ip_address* **[subnetmask** *netmask* **] }**

[no] sgsn multiple-address-group *grp_name* **[disable-gtpc-echo]**
[mcc *mcc_code* **mnc** *mnc_code* **[reject-foreign-subscriber]]**
[plmn-foreign [reject-foreign-subscriber] [rat-type { GAN | GERAN |
HSPA | UTRAN | WLAN }] [description *description* **]**

Web Element Manager Path

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

GGSN Commands - Modified in Release 8.1

The following commands have been modified in Release 8.1.

gtpp dictionary

New dictionaries are available for selection - custom 21 - custom30. The new dictionaries have a default behavior of gtpp dictionary ‘standard’.

CLI (Context Configuration and GTPP Server Group Configuration Modes)

gtpp dictionary {custom1 | custom10 | custom11 | custom12 | custom13 | custom14 | custom15 | custom16 | custom17 | custom18 | custom19 | custom20 | custom21 | custom22 | custom23 | custom24 | custom25 | custom26 | custom27 | custom28 | custom29 | custom3 | custom30 | custom4 | custom5 | custom6 | custom7 | custom8 | custom9 | standard }

default gtpp dictionary

Web Element Manager Path

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

gtpp egcdr

This command configures the parameters and triggers for eG-CDRs. This command has a new keyword set - final-record, with multiple options - to fine-tune the configuration of the final eG-CDRs.

CLI (GTPP Group Configuration Mode)

gtpp egcdr { final-record [closing-cause [same-in-all-partials | unique] | include-content-ids [all | only-with-traffic]] | losdv-max-containers *number* **| lotdv-max-containers** *number* **| service-data-flow threshold [interval** *seconds* **| volume { downlink | total | uplink }** *bytes* **] | service-idle-timeout** *seconds* **}**

Web Element Manager Path

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

gtpu udp-checksum insert

New keyword **default** added to this command and now system sends UDP checksum in outgoing UPD packets by default.

CLI (GGSN Service Configuration Mode)

[no | default } gtpu udp-checksum insert

Web Element Manager Path

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

gtpp storage-server local file

New keyword **purge-processed-files** added in this command to configure the periodic deletion of local processed (*.p) CDR files from the Hard disk on SMC card. This keyword deletes the processed CDR files in every 4 minutes.

CLI (GTPP Group Configuration Mode)

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

default gtpp storage-server local file { compression | format | name | purge-processed-files | rotation }

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

Web Element Manager Path

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

qos rate-limit { downlink | uplink }

New keyword auto-readjust [duration dur] added in this command to configure the burst size dynamically. It also provides different burst size for Peak and Committed data rate-limiting through an APN.

CLI (APN Configuration Mode)

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

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

Web Element Manager Path

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

ipv6 pool

The dup-addr-detection option has been added to the **policy** keyword. This configuration allows an IPv6 shared pool prefix to be shared in multiple call sessions with different interface IDs for an IPv6 address, and duplicate interface IDs are detected.

CLI (Ethernet Port Configuration Mode)

ipv6 pool ***name*** **prefix** ***ip_address/len*** **shared policy dup-addr-detection**

Web Element Manager Path

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

tunnel l2tp

New keyword **local-hostname** *hostname* added to this command to configures the LAC-Hostname AVP to be used for the communication with the LNS peer for an APN.

CLI (APN Configuration Mode)

tunnel l2tp [peer-address *lns-address* **[[encrypted] secret** *l2tp_secret***] [preference** *num***] [tunnel-context** *name***] [local-address** *ip-address***] [crypto-map** *map_name* **{[encrypted] isakmp-secret** *crypto_secret***}] [local-hostname** *hostname***]**

no tunnel [peer-address *lns-address***]**

Web Element Manager Path

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

HA Commands - Modified in Release 8.0

This section provides information on HA commands modified in Release 8.0.

authentication aaa-distributed-mip-keys

New keyword added to **authentication** command in HA Configuration mode to configure the usage of AAA distributed MIP keys for authenticating RRQ for WiMax HA calls.

CLI (HA Configuration Mode)

authentication {aaa-distributed-mip-keys [disabled | optional | required]| imsi-auth | mn-aaa {allow-noauth | always | dereg-noauth | noauth | renew-reg-noauth | renew-and-dereg-noauth} | mn-ha {allow-noauth | always}}

no authentication {aaa-distributed-mip-keys required | imsi-auth}

default authentication [aaa-distributed-mip-keys | imsi-auth | mn-aaa | mn-ha]

Web Element Manager Path

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

HA Commands - Modified in Release 8.1

This section provides information on HA commands modified in Release 8.1.

redirect

This command identifies DNS IP addresses from foreign networks that are to be redirected to the home DNS. A maximum of 16 intercept rules (either redirect or pass-thru) are allow for each intercept list.

Since this command is configured in the source context, the destination context containing the path to the home network DNS is identified using the Context Configuration Mode command ip dns-proxy source-address.

CLI (HA Configuration Mode)

`[ no ] redirect any [ primary-dns ip_address [ secondary-dns ip_address ] ]`

Web Element Manager Path

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

NAT Commands - Modified in Release 8.3

This section provides information on NAT commands modified in Release 8.3.

nat policy

This command enables/disables Network Address Translation (NAT) processing for all subscribers using this rulebase. The optional keyword **`default-nat-realm`** was added to this command. This enables to configure the default NAT realm to be used if one is not already configured.

CLI (Rulebase Configuration Mode)

`nat policy nat-required [ default-nat-realm` *`realm_name`* **`]`**

`{ default | no } nat policy`

Web Element Manager Path

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

PDIF Commands - Modified in Release 8.0

PDIF is not supported in Release 8.0.

PDIF Commands - Modified in Release 8.1

The PDIF commands documented in this section are only available in Release 8.1.

aaa attribute

PDIF decides the radius attributes values and inclusion/exclusion criteria normally through configured radius dictionaries. However, generation of each new dictionary requires a new ST40 PDIF image. The above command is an exception for specifying the required values for the attribute without building a new software image. 3gpp2-serving-pcf is an addition to the existing aaa attribute CLI under PDIF-service config mode.

CLI (Config PDIF Service Config Mode)

[no] aaa attribute 3gpp2-serving-pcf <ip-address>

Web Element Manager Path

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

aaa authentication

Sets the aaa authentication for first and second phase authentication when multiple authentication is configured on the system. Two phase-authentication happens in IKEv2 setup for setting up the IPSec session. The first authentication uses Diameter AAA EAP method and second authentication uses RADIUS AAA authentication. The same AAA context may be used for both authentications. PDIF service allows you to specify only a single AAA group, which could normally be used for the first authentication method.

A given AAA group only supports either Diameter or RADIUS authentication. If the NAI in the first authentication is different from NAI in the second authentication each NAI can point to a different domain profile in the PDIF. Each domain profile may be configured with each AAA group, one for Diameter and the other for RADIUS.

CLI (PDIF Service Config Mode)

aaa authentication { { first-phase | second-phase } |
{ context-name *name* **aaa-group** *name* **} }**
no aaa authentication [first-phase | second-phase]

Web Element Manager Path

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

authentication

The authentication command has a new keyword **gateway** to configure the pre-shared gateway key. The key is either encrypted or clear.

There is also a new keyword **second-phase eap-profile** for installations using multiple authentication and need to configure a second EAP profile

CLI (Crypto Template Config Mode

gateway { encrypted key *value* **| key** *value* **}**
authentication eap-profile *name* **[second-phase eap-profile** *name* **]**

Web Element Manager Path

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

group

PDIF now supports encryption at Diffie-Hellman Group level 14. Selecting any group automatically enables Perfect Forward Secrecy. Selecting the new keyword **none** disables PFS. **none** is the default setting.

CLI (IPsec Transform-set Config Mode)

group *14*

Web Element Manager Path

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

hmac

The **NULL** encryption algorithm represents the optional use of applying encryption within ESP. ESP can then be used to provide authentication and integrity without confidentiality.

CLI (IPsec Transform-Set Config Mode)

hmac *null*

Web Element Manager Path

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

IKEv2-IKESA policy error notification

This modified command in the Crypto-Template config mode generates errors for packets with invalid syntax or invalid message ids.

CLI (Crypto Template Configuration Mode

ikev2-ikesa { keepalive-user-activity | max-retransmissions *number* |
retransmission-timeout *msec* |
**policy error-notification [invalid-message-id | invalid-syntax] |
setup-timer** *sec* | **transform-set list** *name* **}**

Web Element Manager Path

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

peer

The peer command has been amended so the user can administratively enable and disable a Diameter peer. If the peer is disabled, it still retains its configuration. The default option is to Enable.

CLI (Diameter Endpoint Config Mode)

peer *peer_name* **admin-status { enable | disable }**
default peer *peer_name* **admin-status**

Web Element Manager Path

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

proxy-mip

Proxy-MIP command has been extended to include PDIF.

CLI (Subscriber Config Mode)

`proxy-mip required`

Web Element Manager Path

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

server

The start port range for this command has been changed to 45001.

CLI (IPMS Client Config Mode)

`server address ip_address start-port` *`45001`* **`end-port`** *`45005`*

Web Element Manager Path

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

PDSN Commands - Modified for Release 8.0

This section provides information on PDSN commands modified in Release 8.0.

file

New keywords have been added to this command in version 8.0 so unique file sequence numbers can be generated for different rulebase-format-name combinations.

CLI (EDR Configuration Mode/UDR Configuration Mode)

`[ default ] file-sequence-number rulebase-seq-num`

Web Element Manager Path

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

PDSN Commands - Modified for Release 8.1

This section provides information on PDSN commands modified in Release 8.1.

ipv6 pool

The dup-addr-detection option has been added to the **policy** keyword. This configuration allows an IPv6 shared pool prefix to be shared in multiple call sessions with different interface IDs for an IPv6 address, and duplicate interface IDs are detected.

CLI (Ethernet Port Configuration Mode)

ipv6 pool *name* prefix *ip_address/len* shared policy dup-addr-detection

Web Element Manager Path

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

ink aggregation

The auto option has been added to the **rate** keyword. This configuration allows the rate to be set by the peer.

CLI (Ethernet Port Configuration Mode)

link aggregation { master | member | *group N* }
[lacp { active | passive }] [rate { auto | slow | fast }]

Web Element Manager Path

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

clear snmp trap

The cli “clear snmp trap” is updated with new option “statistics”

CLI (Exec Mode Commands)

clear snmp trap { history | statistics }

Web Element Manager Path

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

PDSN Commands - Modified for Release 8.3

This section provides information on PDSN commands modified in Release 8.3.

bcmcs

This command is modified to include new keywords to support ppt.

CLI (PDSN Service Mode Commands)

bcmcs custom ptt {destination-context dest_name | disconnect-dscp-label dscp-label_value| mtu | rohc-profile-name profile_name }

Web Element Manager Path

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

Session Control Manager Commands - Modified for Release 8.0

Session Control Manager is not supported in Release 8.0.

Session Control Manager Commands - Modified for Release 8.1

The following commands have been modified in Release 8.1.

access-type

This **ue-ip-address-range** has been added to specify a UE IP address/range for a specific access type.

CLI (CSCF Service Configuration Mode)

access-type { 3gpp-geran | 3gpp-utran-fdd | 3gpp-utran-tdd | 3gpp2-1x | 3gpp2-1x-hrpd | 3gpp2-umb | adsl | adsl2 | adsl2p | docsis | gshdsl | hdsl | hdsl2 | idsl | ieee-80211 | ieee-80211a | ieee-80211b | ieee-80211g | ieee-80216e | radsl | sdsl | vdsl } access-profile { default | name *access_profile_name* **} | ue-ip-address-range name** *ue_ip_name* **{ address** *ip_address_mask* **| range** *start_ip_address end_ip_address* **}**

no access-type { 3gpp-geran | 3gpp-utran-fdd | 3gpp-utran-tdd | 3gpp2-1x | 3gpp2-1x-hrpd | 3gpp2-umb | adsl | adsl2 | adsl2p | docsis | gshdsl | hdsl | hdsl2 | idsl | ieee-80211 | ieee-80211a | ieee-80211b | ieee-80211g | ieee-80216e | radsl | sdsl | vdsl } [access-profile | ue-ip-address-range [*name ue_ip_name* **]]**

Web Element Manager Path

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

cnsa-media-profile

The **content-type** keyword has been added.

CLI (CSCF Service Configuration Mode)

[no] cnsa-media-profile *profile_id* **cscf-service-policy** *policy_name* **content-type { application-3gpp-ims-xml | application-pidf-diff-xml | application-pidf-partial-xml | application-pidf-xml | application-reginfo-xml | application-sdp | application-xml | message-sipfrag | multipart-mixed | multipart-related | text-plain }**

Web Element Manager Path

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

diameter

The **location-info** keyword has been added to specify the E2-interface for location-information.

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* **]] }**

diameter policy-control { dictionary { Gq-custom | Gq-standard | 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* **]] }**

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

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.

policy

The **threshold congestion-control** keyword has been added to configure the congestion control threshold values that are to be monitored on this CSCF service.

CLI (CSCF Service Configuration Mode)

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

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

Web Element Manager Path

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

trusted-domain-entity

The **foreign-network** keyword has been added to specify that an entity belongs to a Foreign Network.

CLI (CSCF Service Configuration Mode)

trusted-domain-entity *address* **[foreign-network]**

no trusted-domain-entity *address*

Web Element Manager Path

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

SGSN Commands - Modified for Release 8.0

The following commands have been modified in Release 8.0

accounting

The **gtpp group** keyword has been added to this command to associate a defined GTPP group with the SGSN operator policy for accounting (CDR) purposes.

CLI (SGSN Operator Policy Configuration Mode)

accounting context *ctxt_name* **[gtpp group** *grp_name* **]**

Web Element Manager Path

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

accounting

This modified command in the SGSN Service configuration mode provides support for the generation of SMS-types of CDRs for the defined context.

CLI (SGSN Service Configuration Mode)

accounting (cdr-types { s-cdr | m-cdr | sms-mo-cdr | sms-mt-cdr } + | context *ctxt_name* **}**

Web Element Manager Path

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

application-context-name

Three new timer options have been added for configuration of the MAP application contexts.

- mo-fwd-sm
- mt-fwd-sm
- ready-for-sm

CLI (MAP Service Configuration Mode)

application-context-name *application* **operation-timer** *value*
default application-context-name *application* **operation-timer**

Web Element Manager Path

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

authenticate all-event

The **all-event** keyword has been added to the **authenticate** command that all procedures - attaches, service requests, RAUs, detaches, and activations - are to be authenticated for a specific SGSN operator policy.

CLI (SGSN Operator Policy Configuration Mode)

authenticate { activate | all-events | attach | detach | rau | service-request }

Web Element Manager Path

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

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 frequency

The **frequency** keyword has been added to the **authenticate** command to enable the configuration of 1-in-N selective authentication of subscriber events such as attach, RAU, service request, detach, activate primary PDP context requests.

CLI (SGSN Operator Policy Configuration Mode)

authenticate { activate | all-events | attach | detach | rau | service-request } [frequency *frequency* **] [access-type** *gprs* **|** *umts* **]**

default authenticate { activate | all-events | attach | detach | rau | service-request } [frequency]

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.

bind link

For this command, the **nsei** keyword has been changed to be **peer-nsei**

CLI (Port Channelized Configuration Mode)

bind link peer-nsei nse_id *245* **ns-vci ns-vc_id** *5555*

Web Element Manager Path

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

cc profile

This modified command defines an instance of the CC profile with the charging triggers, configured with modified keywords, the SGSN will use to generate various types of CDRs for the SGSN service.

CLI (GPRS Service Configuration Mode)

cc profile *profile_bits* **[buckets** *number* **| interval** *time* **| tariff time1** *mins hours* **[time2** *mins hours* **] [time3** *mins hours* **] [time4** *mins hours* **] | volume { downlink** *down_vol* **uplink** *up_vol* **| total** *total_vol* **}] +**

Web Element Manager Path

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

ciphering-algorithm

Default value has been changed so that the user has more control over when ciphering is performed. The new default value is gea0, no ciphering.

CLI (GPRS Service Configuration Mode)

default ciphering-algorithm priority *priority*

Web Element Manager Path

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

clear subscriber

New filter keyword **nsapi** added to this existing command to clear the subscriber and session information on the basis of network service access point identifier (NSAPI).

CLI (Exec Mode)

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

Web Element Manager Path

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

equipment-identity-register

New filter keyword **check-imei-every-n-events** added to this existing command to set the frequency (1-in-N) of sending 'check IMEI' messages to the EIR. This reduces EIR-SGSN traffic.

CLI (MAP Service Configuration Mode)

equipment-identity-register { isdn *E.164_num* **| point code** *pt_code* **}**
[source-ssn *ssn* **| check-imei-every-n-events** *times* **]**

Web Element Manager Path

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

frame-relay

This command configures the parameters for the Frame Relay connection, including the fractional channel.

CLI (Channelized Port Configuration Mode)

frame-relay path path_id { ds1 *connects* **| e1** *connects* **}**
timeslots *slot#* **[intf-type** *intf_type* **] [lmi_type** *lmi_type* **]**

Web Element Manager Path

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

gmm

In this command, new timers have been added:

- mobile-reachable-timeout - range 4 to 1440 minutes, default 58 minutes
- purge-timeout - range 1 to 20160, default 10080 minutes

In this command, timers have been given default values:

- t3302-timeout - default 12 minutes
- t3312-timeout - default 54 minutes
- t3313-timeout - default 5 seconds
- t3314-timeout - default 44 seconds
- t3350-timeout - default 6 seconds
- t3360-timeout - default 6 seconds
- t3370-timeout - default 6 seconds

In this command, some timers have been modified:

- 't3314-negotiate-timeout' is now 'negotiate-t3314-timeout'
- 'llc pdu-lifetime' timer has been moved to the **llc** command

In this command, some timers have been removed:

- t3322-timeout
- implicit-detach-timeout
- max-auth-retransmission
- max-identity-retransmission

- max-page-retransmission
- perform-identity-on-auth-failure
- ptmsi-reallocate

CLI (GPRS Service Configuration Mode)

[default] gmm { mobile-reachable-timeout mins | negotiate-t3314-timeout secs | purge-timeout mins | T3302-timeout mins | T3312-timeout mins | T3313-timeout secs | T3350-timeout secs | T3360-timeout secs | T3370-timeout secs } +

Web Element Manager Path

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

gmm

TP PR 7549; ST16 PR 110911

The **negotiate-t3314-timeout** keyword has been modified in two way:

- the maximum value for this timer has increased to 11160.
- the behavior of this timer has changed when it is disabled, so that by disabling negotiation of the T3314-timeout value, if the MS sends the requested value of the ready timer in the Att/RAU Request, then the SGSN sends the T3314-timeout value in the Att/RAU Accept.

CLI (GPRS Service Configuration Mode)

[no | default] gmm negotiate-t3314-timeout [*<0-11160> seconds* **]**

Web Element Manager Path

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

gtpp

This existing command is now available for SGSN service in Context configuration mode for mentioned variants to configure Ga interface for accounting in SGSN service.

CLI (Context Configuration Mode)

gtpp charging-agent address
gtpp duplicate-hold-time minutes
gtpp echo-interval
gtpp max-cdrs
gtpp max-pdu-size
gtpp max-retries
gtpp redirection-allowed
gtpp server
gtpp storage-server
gtpp timeout

Web Element Manager Path

Configuration of these features is not yet supported by the Web Element Manager.

gtpp dictionary

This command designates specific dictionary used by GTPP for specific context. New dictionaries were added to this command.

CLI (Context Configuration and GTPP Server Group Configuration Modes)

gtpp dictionary { custom1 | custom10 | custom11 | custom12 | custom13 | custom14 | custom15 | custom16 | custom17 | custom18 | custom19 | custom2 | custom20 | custom3 | custom4 | custom5 | custom6 | custom7 | custom8 | custom9 | standard }

default gtpp dictionary

Web Element Manager Path

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

gtpp interim now

This command check points current GTPP accounting messages and identifies which types of interim CDRs are to be generated and sent to the external charging/storage servers (e.g., a CFG or a GSS). The impact of this command is immediate. The following keywords have been added to assist with fine tuning the GTPP messages:

- callid
- cdr-types
- dhcp-server
- gprs-service
- mcc/mnc
- msisdn
- sgsn-service

CLI (Exec Mode)

gtpp interim now [active-charging egcdr | apn *apn_name* **| callid** *call_id* **| cdr-types { mcdr | scdr } | dhcp-server** *ip_address* **| gprs-service** *svc_name* **| ggsn-service** *svc_name* **| imsi** *imsi* **[ip-address sub_address [username** *name* **] now | nsapi** *nsapi* **[ip-address** *sub-address* **[username** *name* **] | username** *name* **]] | ip-address** *sub_address* **[username** *name* **] | ip-pool** *pool_name* **| mcc** *mcc_number* **mnc** *mnc_number* **| msisdn** *msisdn_num* **| sgsn-address** *ip_address* **| sgsn-service** *svc_name* **| username** *name* **] +**

Web Element Manager Path

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

gtpp max-cdrs

TP PR 4360 ST16 PR 70569

The **default** keyword was added to the syntax.

CLI (GTPP Group Configuration Mode)

[default] gtpp max-cdrs *number* **[wait-time** *seconds* **]**

Web Element Manager Path

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

gtpp trigger

The **plmn-id-change** keyword has been added to this command to enable the PLMN-ID-change trigger for S-CDRs if the dictionary specified in the **gtpp dictionary** configuration supports the PLMN-ID change. If enabled, the SGSN generates a partial S-CDR when the MS changes the PLMN while under the same 2G SGSN. Currently, custom18 dictionary supports this trigger.

CLI (GTPP Group Configuration Mode)

```
[ no ] gtpp trigger plmn-id-change
default gtpp trigger
```

Web Element Manager Path

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

lawful-intercept

Two new keywords, **interception-point-policy (sms-mt or sms-mo)** and **reprovision-target-policy resend-pdp-context-active-iri** have been added to the **lawful-intercept** command for use with an SGSN license to support interception of SMS messages.

CLI (Global Configuration Mode)

```
lawful-intercept { acked-udp [ num-retry number ] [ timeout time ] |
hand-off-policy send-start-intercept-with-pdp-active-iri |
interception-point-policy { { sms-mo | sms-mt } { message-delivered |
request-received } } | reprovision-target-policy
resend-pdp-context-active-iri | src-ip-addr ip_address | tcp tcp_option |
unack-format use-service-address }
```

Web Element Manager Path

Configuration of these features is not yet supported by the Web Element Manager.

lawful-intercept

A new keyword, **hand-off-policy send-start-intercept-with-pdp-active-iri,** has been added to the **lawful-intercept** command for use with an SGSN license to enable/disable configuration to send ‘start intercept’ messages in the event of an ISRAU.

CLI (Global Configuration Mode)

```
lawful-intercept { acked-udp [ num-retry number ] [ timeout time ] |
hand-off-policy send-start-intercept-with-pdp-active-iri |
interception-point-policy { { sms-mo | sms-mt } { message-delivered |
request-received } } | reprovision-target-policy
resend-pdp-context-active-iri | src-ip-addr ip_address | tcp tcp_option |
unack-format use-service-address }
```

Web Element Manager Path

Configuration of these features is not yet supported by the Web Element Manager.lawful-intercept

A new keyword, **tcp,** has been added to the **lawful-intercept** command for use with an SGSN license to enable use of the TCP interface in place of the UPD interface. The new keyword includes timer and addressing options.

CLI (Global Configuration Mode)

lawful-intercept { acked-udp [num-retry number] [timeout time] | hand-off-policy send-start-intercept-with-pdp-active-iri | interception-point-policy { { sms-mo | sms-mt } { message-delivered | request-received } } | reprovision-target-policy resend-pdp-context-active-iri | src-ip-addr ip_address | tcp { [application-heartbeat-messages timeout *time* **] | [connection-retry-timer** *time* **] | [content-delivery { dest-addr** *ipv4_add* **dest-port** *port* **}] [event-delivery { dest-addr** *ipv4_add* **dest-port** *port* **}] | unack-format use-service-address }**

Web Element Manager Path

Configuration of these features is not yet supported by the Web Element Manager.

llc

The **pdu-lifetime** parameter has been moved from the **gmm** command in the GPRS Service Configuration Mode to the **llc** command in the same mode and the parameter's default has been changed from 60 seconds to 6 seconds. As well, all the t200 timer names have been simplified.

CLI (GPRS Service Configuration Mode)

llc { 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 **iov-ui-in-xid-reset** keyword has been added to the **llc** command to allow the operator to configure whether or not the SGSN sends IOV-UI in XID-RESET messages. The SGSN sends the IOV-UI by default.

CLI (GPRS Service Configuration Mode)

llc { iov-ui-in-xid-reset | 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 **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.

map

This existing command is now enhanced with new keyword **imeisv** to include the International Mobile Equipment Identity-Software Version (IMEI-SV) information to include in GPRS Location Update (GLU) request message.

CLI (SGSN Operator Policy Configuration Mode)

[remove] map message update-gprs-location [private-extension access-type | imeisv]

Web Element Manager Path

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

network-service-entity ip

This command has been modified. See network-service-entity

network-service-entity

The **network-service-entity frame-relay** and **network-service-entity ip** commands have been combined under this new command name - **network-service entity**.

This command has two keyword options:

ip-local - to create an NSE instance within an IP environment and enter NSE-IP configuration mode, a sub-mode of the Global Configuration Mode . The Network Service

Entity - IP mode enables you to configure the management functionality for the Gb interface between a BSS and an SGSN over a 2.5G GPRS IP network connection. This configuration mode includes the following commands.

- max-ns-retransmissions
- ns-timer
- nsvc-failure-action
- nsvl

peer-nsei - to create an NSE instance within a Frame Relay environment and enter the NSE-FR configuration mode, a sub-mode of the Global Configuration mode. The NSE-FR configuration mode enables you to define and manage the functionality for the Gb interface between a BSS and an SGSN over a 2.5G GPRS frame relay network connection. This configuration mode includes the following command:

- **nsvc** to create a network service virtual connection instance and enter the NSVC configuration mode.

CLI (Global Configuration Mode)

[no] network-service-entity (ip-local | peer-nsei *peer-nsei* **frame-relay}**

Web Element Manager Path

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

network-service-entity ip-local

A new keyword - **all-nsvc-failure-action** - has been added to this command to configure how the SGSN handles the NSE when NSVC, connected to the BSC, go down. Options include:

- clear-nse which instructs the SGSN to SGSN to clear NSE if all NSVC to the BSC are down.
- default which means the NSE is not cleared if all NSVC go down.

CLI (Network Service Entity IP Local Configuration Mode)

all-nsvc-failure-action clear-nse

default all-nsvc-failure-action

Web Element Manager Path

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

nri

Two new keywords - **null-nri-value** and **non-broadcast lac/rac** - have been added to this command to facilitate the SGSN off loading procedure which is part of Gb flex (SGSN) pooling.

CLI (GPRS Service Configuration Mode)

nri length *length* **null-nri-value** *null_nri_value* **non-broadcast lac** *lac_id* **rac** *rac_id* **nri-value** *nri_value*

no nri

Web Element Manager Path

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

ns-timer

The default value of the **test** keyword for the **ns-timer** command has been increased from 5 to 30 seconds:

CLI (Network Service Entity IP Local Configuration Mode)

ns-timer test <*time*>

Web Element Manager Path

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

ns-vc

The command creates Network Service Virtual Connection Configuration sub-mode in the Network Service Entity Frame Relay configuration mode to define the management functionality for a specific network service virtual connection of the Gb interface between a BSS and an SGSN in a 2.5G GPRS frame relay network connection.

- **retries** - command has been deprecated
- **timer** - command has been deprecated

CLI (Network Service Entity - Peer NSEI Configuration Mode)

[no] ns-vc instance *nsvc_id*

Web Element Manager Path

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

nsvl

This command name has been modified - it was originally **ns-vl** - it is now **nsvl**. Nothing else about this command has changed.

The command creates Network Service Virtual Link Configuration sub-mode in the Network Service Entity IP configuration mode to define the management functionality for a specific network service virtual link in a 2.5G GPRS IP network connection.

CLI (Network Service Entity - IP Configuration Mode)

[no] nsvl instance *nsvl_id*

Web Element Manager Path

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

nsvl-address

The following keywords in this command have been deprecated and the functionality has been moved into a separate command in this configuration mode, command **weight**.

- signaling weight
- data weight

CLI (NSVL Configuration Mode)

Web Element Manager Path

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

paging-policy

The command name has changed from paging-scheme to paging policy but it still configures the paging parameters for the GPRS service. Keywords (parameters) have been modified and combined to enhance efficiency:

CLI (GPRS Service Configuration Mode)

paging-policy { last-known-area { all | bsc | cell | location-area | routing-area } | max-retransmissions *retran_num* **}**

Web Element Manager Path

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

paging-policy

With the addition of the zero (‘0’) to the value range for the **max-retransmissions** keyword, it is now possible to disable retransmissions for paging policy so only a single 2G PS-paging request will be sent to the BSC.

CLI (GPRS Service Configuration Mode)

paging-policy { last-known-area { all | bsc | cell | location-area | routing-area } | max-retransmissions < *0 to 5* >**}**

Web Element Manager Path

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

partial-apn-match

New keyword (**partial-apn-match**) has been added to the **sm** command to optimize radio resource usage by managing signaling between the MS and the SGSN. Specifically, this keyword enables partial matching of a requested APN during APN selection.

CLI (GPRS Service Configuration Mode)

sm { activate-max-retransmissions num_retries | deactivate-max-retransmissions num_retries | ignore-pco-decode-error | modify-max-retransmissions num_retries | partial-apn-match | requested-apn-from-first-subrec | t3385-timeout secs | t3386-timeout secs | t3395-timeout secs | trim-trailing-spaces-in-apn }

Web Element Manager Path

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

peer-nsei

This command was the nsei command in the GPRS service configuration mode. The command now has a new name.

This command has a new keyword - **pooled** - which enables pooling with non-pooled BSCs within the pool area.

CLI (GPRS Service Configuration Mode)

peer-nsei *nse_id* **{ lac** *lac_id* **rac** *rac_id* **| pooled }**

[no] peer-nsei *nse_id* **{ lac** *lac_id* **rac** *rac_id* **| pooled }**

Web Element Manager Path

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

qos class

The MBR and GBR downlink rates, part of the qualifying options configuration, for all four QoS classes have been increased to 256000 kbps.

CLI (SGSN APN Configuration Mode)

qos class { background | conversational | interactive | streaming } [*qualif_option* **]**

Web Element Manager Path

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

qos class

Existing CLIs keywords value options have been modified to support the HSUPA+ in the SGSN.

CLI (SGSN APN Configuration Mode)

qos class background mbr-up <1…256000kbps>

qos class conversational mbr-up <1…256000kbps>

qos class conversational gbr-up <1…256000kbps>

qos class interactive mbr-up <1…256000kbps>

qos class streaming mbr-up <1…256000kbps>

qos class streaming gbr-up <1…256000kbps>

Web Element Manager Path

This functionality 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.

rau-inter

This new CLI keyword enables the operator to configure the GMM cause code that will be included in the Routing Area Update Reject message sent to the MS when the peer SGSN address resolution process fails during Inter SGSN RAU.

CLI (SGSN Operator Policy Configuration Mode)

```
rau-inter peer-sgsn-addr-resolution-failure failure-code { 9 | 10 }
```

Web Element Manager Path

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

requested-apn-from-first-subrec

This new keyword for the **sm** command enables use of a ‘requested APN’ from the first subscription record.

CLI (GPRS Service Configuration Mode)

```
[ default | no ] sm requested-apn-from-first-subrec
```

Web Element Manager Path

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

sgsn-context-request

The word 'allowed' has been removed from the default form of this command.

CLI (GPRS Service Configuration Mode)

```
default sgsn-context-request ptmsi-signature-absence
```

Web Element Manager Path

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

show session

The words **gprs-only** and s**gsn-only** have been added to various show session commands to limit output to MM and PDP context information.

CLI (Exec Configuration Mode)

```
show session disconnect-reasons [ gprs-only | sgsn-only ]
show session duration [ gprs-only | sgsn-only ]
show session setuptime [ gprs-only | sgsn-only ]
```

Web Element Manager Path

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

sm

A new keyword has been added to the **sm** command, **ignore-pco-decode-error**. This option enables the SGSN to ignore received decode errors that are due to incorrectly encoded PCO IE length in SM Requests.

CLI (GPRS Service Configuration Mode)

```
sm ignore-pco-decode-error
default sm ignore-pco-decode-error
```

Web Element Manager Path

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

trim-trailing-spaces-in-apn

New keyword (**trim-trailing-spaces-in-apn**) has been added to the **sm** command to optimize radio resource usage by managing signaling between the MS and the SGSN. Specifically, this keyword enables the SGSN to strip off any trailing space(s) in the requested APN.

CLI (GPRS Service Configuration Mode)

```
sm { activate-max-retransmissions num_retries | deactivate-max-
retransmissions num_retries | ignore-pco-decode-error |
modify-max-retransmissions num_retries | partial-apn-match |
requested-apn-from-first-subrec | t3385-timeout secs | t3386-timeout secs |
t3395-timeout secs | trim-trailing-spaces-in-apn }
```

Web Element Manager Path

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

SGSN Commands - Modified for Release 8.1

The following commands have been modified in Release 8.1

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.

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.

frame-relay

This command configures the parameters for the Frame Relay connection, including the fractional channel.

CLI (Channelized Port Configuration Mode)

frame-relay path path_id { ds1 *connects* **| e1** *connects* **}**
timeslot *slot#* **[intf-type** *intf_type* **] [lmi_type** *lmi_type* **]**

Web Element Manager Path

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

gtpp storage-server local file

New keyword **purge-processed-files** added in this command to configure the periodic, every 4 minutes, deletion of local processed (*.p) CDR files from the hard disk on SMC card.

CLI (GTPP Group Configuration Mode)

gtpp storage-server local file { compression { gzip | none } | format { custom1 | custom2 | custom3 | custom4 | custom5 } | name prefix *prefix* **|**

purge-processed-files | rotation { cdr-count *count* **| time-interval** *time* **| volume** *size* **} }**

default gtpp storage-server local file { compression | format | name | purge-processed-files | rotation }

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

Web Element Manager Path

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

gtpc

Keyword ignore response-port-validation has been added to this command to instruct the SGSN to ignore the response port validation.

CLI (SGTP Service Configuration Mode)

gtpc ignore response-port-validation

Web Element Manager Path

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

imsi

The keyword **imsi** has been added to the **imsi** command to enable the IMSI (E.212 address) to be used as the destination address in the HLR configuration.

CLI (HLR Configuration Mode)

imsi { any | starts-with *prefix_number* **} { imsi [sgsn-source-address-format point-code-ssn [source-ssn** *ssn* **] | isdn** *isdn_number* **| mobile-global-title** *mgt_number* **| point-code** *pt-code* **} }**

Web Element Manager Path

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

imsi

The functionality of this keyword has been modified so that it enables configurable default behavior for routing.

- Entering imsi with the any keyword preserves the default behavior and the E.212 address is used as a destination address and the MAP request will be sent towards the HLR.
- If this keyword is not used with the any keyword, then the MAP request will be rejected.

CLI (HLR Configuration Mode)

imsi { any | starts-with *prefix_number* **} { imsi [sgsn-source-address-format point-code-ssn [source-ssn** *ssn* **] | isdn** *isdn_number* **| mobile-global-title** *mgt_number* **| point-code** *pt-code* **} }**

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.

nri length

The non-broadcast keyword in this command has been modified to include the values of the PLMN's MCC and MNC to enable support for multiple IuPS Services when Iu-Flex is utilized.

CLI (SGSN APN Configuration Mode)

nri length *nri_length* **{ nri-value** *nri_value* **| null-nri-value** *null_nri_value* **non-broadcast mcc** ***mcc*** **mnc** ***mnc*** **lac** *lac_id* **rac** *rac_id* **[nri-value** *value* **}**

Web Element Manager Path

This functionality 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.

qos rate-limit

Keyword **auto-readjust** and keyword **duration** have been added as options to the **burst-size** keyword to expand functionality and provide dynamic burst-size calculation support for traffic policing.

- **readjust** : This keyword enables dynamic burst-size calculation support for traffic policing.
- **duration** <*seconds*> : Must be an integer from 1 to 30. This keyword sets the number of seconds that the dynamic burst-size calculation will last.

CLI (SGSN APN Configuration Mode)

qos rate-limit direction { downlink | uplink } [burst-size { auto-readjust [duration <*seconds*>] | <*bytes*> }]

qos rate-limit direction { downlink | uplink } class <*traffic-class*> [burst-size { auto-readjust [duration <*seconds*>] | <*bytes*> }]

Web Element Manager Path

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

radio-network-controller

The **radio-network-controller** command has been changed to make it easier for the operator to enter the command. The new command to create an RNC configuration instance is **rnc**. Identification of the MCC and MNC are no longer associated with the configuration instance.

CLI (IuPS Service Configuration Mode)

rnc *rnc_id*

Web Element Manager Path

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

ranap allocation-retention-priority-ie

This command configures the parameters for the allocation-retention-priority (ARP) IE inserted in the RAB assignment request message.

CLI (SGSN APN Configuration Mode)

ranap allocation-retention-priority-ie subscription-priority *priority* **class { { background | conversational | interactive | streaming } { not-pre-emptable | priority | queuing-disallowed | shall-not-trigger-pre-emptable } + }**

[default | remove | no] ranap allocation-retention-priority-ie [subscription-priority *priority* **class { background | conversational | interactive | streaming }]**

Web Element Manager Path

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

routing-context

For releases 8.1 and higher, the range of values for this keyword has been increased from maximum of 65535 to 4294967295 in accordance with RFC 4666.

CLI (SS7 Routing Domain Configuration Mode)

routing-context < 1 - 4294967295**>**

Web Element Manager Path

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

Obsoleted Commands

Common Commands - Obsoleted in Release 8.0

This section provides information on commands that are common to all products that were obsoleted in Release 8.0.

context-cleanup-period

Removed and replaced in functionality by **`context-timeout`** *`seconds`*

CLI (ROHC-Profile Decompress-Config Mode

`context-cleanup-period` *`variable`*

Web Element Manager Path

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

diameter dictionary

This command is deprecated. The Diameter dictionaries for accounting and authentication can now be configured using the **`diameter accounting dictionary`** and **`diameter authentication dictionary`** commands.

CLI (AAA Server Group and Context Configuration Modes)

`diameter dictionary { aaa-custom1 | aaa-custom10 | aaa-custom2 | aaa-custom3 | aaa-custom4 | aaa-custom5 | aaa-custom6 | aaa-custom7 | aaa-custom8 | aaa-custom9 | nasreq | rf-plus }`

`[ default ] diameter dictionary`

Web Element Manager Path

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

fragment-size

The **`fragment-size`** command has been removed from DLCI Configuration Mode.

CLI (DLCI Configuration Mode Commands)

[default] fragment-size *`number`*

header-type

The **`header-type`** command has been removed from DLCI Configuration Mode.

CLI (DLCI Configuration Mode Commands)

header-type { 2byte | 4byte }

`[ default ] header-type`

service-type

The **pwe3-cseopsn** keyword has been obsoleted and replaced with the **mtp2** keyword.

CLI (Card Configuration Mode)

service-type { frame-relay | pwe3-cesopsn | mtp2 | unspecified }

Web Element Manager Path

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

tx-priority

The **tx-priority** command has been removed from DLCI Configuration Mode.

CLI (DLCI Configuration Mode Commands)

tx-priority *priority*

[default] tx-priority

vc-mapping

The **vc-mapping** command has been deprecated and removed from the Channelized Port Configuration Mode. Frame mapping is now completely standards compliant and done through **path** command configuration explained in the *Channelized Port Configuration Mode* chapter in the *Command Line Interface Reference*.

CLI (Channelized Port Mode Commands)

vc-mapping { g.707 | interleaved }

{ deny | permit } [log] { tcp | udp }

Removed "**treatment { conversational | streaming | background | interactive-1 | interactive-2 | interactive-3}**" keyword from this command:

CLI (ACL Configuration Mode and IPv6 ACL Configuration Mode)

{ deny | permit } [log] { tcp | udp } { { source_address source_wildcard | any | host source_host_address } [eq source_port | gt source_port | lt source_port | neq source_port] } { { dest_address dest_wildcard | any | host dest_host_address } [eq dest_port | gt dest_port | lt dest_port | neq dst_port] | treatment { conversational | streaming | background | interactive-1 | interactive-2 | interactive-3}}

Common Commands - Obsoleted in Release 8.1

This section provides information on commands that are common to all products that were obsoleted in Release 8.1.

enable/disable super-charger

This command has been deprecated and replaced with the super-charger command in the SGSN Operator Policy configuration mode.

CLI (SGSN Service Configuration Mode)

enable | disable super-charger

isakmp disable-phase1-rekey

This command deprecated and replaced with **`ikev1 disable-phase1-rekey`** command.

CLI (Context Configuration Mode)

`[ no ] isakmp disable-phase1-rekey`

Web Element Manager Path

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

isakmp keepalive

This command deprecated and replaced with **`ikev1 keepalive dpd`** command.

CLI (Context Configuration Mode)

`[ no ] isakmp keepalive dpd interval` *`interval`* **`timeout`** *`time`* **`num-retry`** *`retries`*

Web Element Manager Path

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

isakmp policy

This command deprecated and replaced with **`ikev1 policy`** command.

CLI (Context Configuration Mode)

`[ no ] isakmp policy` *`priority`*

Web Element Manager Path

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

CF Commands - Obsoleted in Release 8.0

This section provides information on CF commands that were obsoleted in Release 8.0.

timeout action

This command is deprecated and replaced with the **`failure-action`** command.

CLI (Content Filtering Server Group Configuration Mode)

`timeout action { allow | content-insertion` *`content_string`* **`| discard | redirect-url`** *`url`* **`| terminate-flow }`**

`default timeout action`

Web Element Manager Path

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

CF Commands - Obsoleted in Release 8.1

timeout action

This command is deprecated and replaced by the **`failure-action`** command.

CLI (Content Filtering Policy Configuration Mode)

`timeout action { allow | content-insert` *`content_string`* **`| discard | redirect-url`** *`url`* **`| terminate-flow | www-reply-code-and-terminate-flow`** *`reply_code`* **`} [ edr`** *`edr_format_name`* **`]`**

`default timeout action [ edr` *`edr_format_name`* **`]`**

Web Element Manager Path

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

ECS Commands - Obsoleted in Release 8.0

This section provides information on ECS commands that were obsoleted in Release 8.0.

tcp out-of-order-timeout

This command is deprecated and replaced with the **`tcp packets-out-of-order`** command.

CLI (Rulebase Configuration Mode)

`tcp out-of-order-timeout` *`timeout`*

Web Element Manager Path

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

wtp out-of-order-timeout

This command is deprecated and replaced with the **`wtp packets-out-of-order`** command.

CLI (Rulebase Configuration Mode)

`wtp out-of-order-timeout` *`duration_ms`*
`default wtp out-of-order-timeout`

Web Element Manager Path

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

ECS Commands - Obsoleted in Release 8.1

This section provides information on ECS commands that were obsoleted in Release 8.1.

bearer apn

This command defines a rule definition to analyze and charge user traffic based on APN bearer. In StarOS 8.1 and later, this command is deprecated and is replaced by the **bearer 3gpp apn** command.

CLI (Ruledef Configuration Mode)

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

Web Element Manager Path

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

bearer imsi

This command defines a rule definition to analyze and charge user traffic based on International Mobile Station Identification number (IMSI) in bearer flow. In StarOS 8.1 and later, this command is deprecated and is replaced by the bearer **3gpp imsi** command.

CLI (Ruledef Configuration Mode)

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

Web Element Manager Path

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

bearer rat-type

This command defines a rule definition to analyze and charge user traffic based on the Radio Access Technology (RAT) in bearer flow. In StarOS 8.1 and later, this command is deprecated and is replaced by the **bearer 3gpp rat-type** command.

CLI (Ruledef Configuration Mode)

[no] bearer rat-type *operator rat*

Web Element Manager Path

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

bearer sgsn-address

This command defines a rule definition to analyze and charge user traffic based on SGSN address associated in bearer flow. This command is deprecated and replaced by the **bearer 3gpp sgsn-address** command.

CLI (Ruledef Configuration Mode)

[no] bearer sgsn-address *operator address*

Web Element Manager Path

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

Firewall Commands - Obsoleted in Release 8.0

No Firewall commands were obsoleted from Release 8.0.

Firewall Commands - Obsoleted in Release 8.1

This section provides information on Firewall commands that were obsoleted in Release 8.1.

firewall policy

This command enables/disables Stateful Firewall support for subscriber/APN. This configuration is now available in the Rulebase Configuration mode.

CLI (APN and Subscriber Configuration Modes)

```
firewall policy firewall-required
{ default | no } firewall policy
```

Web Element Manager Path

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

GGSN Commands - Obsoleted in Release 8.0

This section provides information on GGSN commands that were obsoleted in Release 8.0.

qos traffic-policing

This command is deprecated and replaced with traffic shaping related commands:

- **qos negotiate-limit**
- **qos rate-limit**

qos-renegotiation

This command is deprecated for GGSN service from APN configuration mode and Subscriber Configuration Mode. Dynamic QoS renegotiation support is now in Enhanced Charging Service configuration.

CLI (APN Configuration Mode and Subscriber Configuration Mode)

[no | default] qos-renegotiate

timeout

Keyword **qos-renegotiate** *time* is removed from this command for GGSN service from APN configuration mode and Subscriber Configuration Mode. Dynamic QoS renegotiation support is now in Enhanced Charging Service configuration.

CLI (APN Configuration Mode and Subscriber Configuration Mode)

[no | default] timeout qos-renegotiate *time*

Web Element Manager Path

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

GGSN Commands - Obsoleted in Release 8.1

No GGSN commands were obsoleted from Release 8.1.

HA Commands - Obsoleted in Release 8.0

No HA commands were obsoleted from Release 8.0.

HA Commands - Obsoleted in Release 8.1

No HA commands were obsoleted from Release 8.1.

PDSN Commands - Obsoleted in Release 8.0

No PDSN commands were obsoleted from Release 8.0.

PDSN Commands - Obsoleted in Release 8.1

No PDSN commands were obsoleted from Release 8.1.

Session Control Manager Commands - Obsoleted in Release 8.0

Session Control Manager is not supported in Release 8.0.

Session Control Manager Commands - Obsoleted in Release 8.1

This section provides information on SCM commands that were obsoleted in Release 8.1.

access-network

This command configures the location specific mobile network identifiers used to match location specific emergency/service numbers.

CLI (CSCF Proxy-CSCF Configuration Mode)

access-network mcc *code* **mnc** *code*

no access-network

Web Element Manager Path

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

SGSN Commands - Obsoleted in Release 8.0

The following commands have been obsoleted during the development cycle of Release 8.0

Gs Service Configuration Mode

The following commands have been removed from this configuration mode:

CLI (Gs Service Configuration Mode)

- **T10-timeout**
- **T12-1-timeout**
- **T12-2-timeout**
- **T6-1-timeout**
- **T8-timeout**
- **T9-timeout**
- **access-protocol**
- **location-area-code-list**
- **max-N10-retransmission**
- **max-N12-retransmission**
- **max-N8-retransmission**
- **max-N9-retransmission**
- **vlr-hash**

NSE-FR Configuration Mode

The following command has been obsoleted:

- **bssgp-timer**

NSE-IP Configuration Mode

The following commands have been obsoleted or replaced:

- **peer-network-service-entity**
- **retry-count**
- **timer**

Replacement commands have been documented in the *NSE-IP Configuration Mode* chapter of the *CLI Reference Guide.*

SGSN Operator Policy Configuration Mode

The following command has been obsoleted:

- **charging context**

Replacement commands have been documented in the *CLI Reference Guide*.

SGSN Service Configuration Mode

The following commands have been removed from this configuration mode:

CLI (SGSN Service Configuration Mode)

- **page-timer**
- **path-failure**
- **periodic-ra-upd-timer**
- **plmn**
- **purge-timer**

SGSN Commands - Obsoleted in Release 8.1

No SGSN commands were obsoleted from Release 8.1.

GTPP Storage Server (GSS)

This section documents additions and modifications to the GSS.

GSS Changes in Release 8.0

None for this release.

GSS Changes in Release 8.1

None for this release.

Web Element Manager Changes

This section documents additions and modifications to the Web Element Manager.

No changes were made for this release.

CHAPTER 4
ACCOUNTING MANAGEMENT

This section contains additions and changes made to the accounting-related parameters available in Release 8.0 unless specifically designated as being in Release 8.1.

Bulk Statistic Enhancements in Release 8.0

This section lists bulk statistic additions and changes in Release 8.0. Detailed information on bulk statistics is located in both the *System Administration Guide* and in the *Statistics and Counters Reference*.

Bulk Statistic Additions

Support for the following bulk statistics has been added:

Context Schema

The following are new for Release 8.0:

- sfw-total-dosattacks
- sfw-total-flows
- sfw-total-injectedbytes
- sfw-total-injectedpkts

gprs schema

The following are new for Release 8.0:

- sns-config-fail-rcv-prot-err-unspec
- sns-config-fail-sent-prot-err-unspec
- sns-config-fail-rcv-inval-essential-param
- sns-config-fail-sent-inval-essential-param
- sns-add-fail-rcv-prot-err-unspec
- sns-add-fail-sent-prot-err-unspec
- sns-add-fail-rcv-inval-essential-param
- sns-add-fail-sent-inval-essential-param
- num-sns-delete-rcvd
- sns-delete-fail-rcv-prot-err-unspec
- sns-delete-fail-sent-prot-err-unspec
- sns-delete-fail-rcv-inval-essential-param
- sns-delete-fail-sent-inval-essential-param
- num-sns-cw-rcvd
- sns-cw-fail-rcv-prot-err-unspec
- sns-cw-fail-sent-prot-err-unspec
- sns-cw-fail-rcv-inval-essential-param
- sns-cw-fail-sent-inval-essential-param
- bssgp-flush-llc-msg-sent
- bssgp-flush-llc-ack-msg-rcvd
- bssgp-cs-paging-msg-sent
- bssgp-ps-paging-msg-sent

- bssgp-pkt-drop-flow-ctrl-queue-full
- bssgp-downlink-pkt-drop
- bssgp-bvc-unknown-ms-status-msg-rcvd
- bssgp-bvc-unknown-ms-status-msg-sent
- sndcp-xid-req-ms-init
- sndcp-xid-ind-sgsn-init
- sndcp-npdus-ack-rcvd-ms
- sndcp-npdus-ack-sent-ms
- sndcp-npdus-uack-rcvd-ms
- sndcp-npdus-uack-sent-ms
- sndcp-bytes-ack-rcvd-ms
- sndcp-bytes-ack-sent-ms
- sndcp-bytes-uack-rcvd-ms
- llc-data-sent-ind-tx
- llc-frame-stats-ui-tx
- llc-frame-stats-ui-ciph-rx
- llc-frame-stats-ui-ciph-tx
- llc-frame-stats-octets-rcvd
- llc-frame-stats-octets-sent
- llc-frame-stats-unack-frames-rcvd
- llc-frame-stats-unack-frames-sent
- llc-frame-stats-xid-rcvd
- llc-frame-stats-xid-sent
- packets-sent-to-bsc
- packets-rcvd-from-bsc
- bytes-sent-to-bsc
- bytes-rcvd-from-bsc
- 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

gtpc schema

- err-ind-rx-discard
- num-dt-recv-err-ind

- sri-req

gtpp schema

- mgmt-int-close

sccp schema

- sccp-reassem-err-timer
- sccp-reassem-err-sequence
- sccp-reassem-err-space
- sccp-err-msg-rcvd
- sccp-unequipped-user
- sccp-reason-unknown
- sccp-congested-msg-rcvd
- sccp-prohibit-msg-rcvd

sgsn schema

The following are new for Release 8.0:

- gprs_standby
- gprs_ready
- 2G-rau-accept-intra
- 3G-ret-rau-accept-periodic
- 2G-ret-rau-accept-periodic
- 3G-ms-init-detach
- 2G-ms-init-detach
- 3G-ms-init-imsi-detach
- 2G-ms-init-imsi-detach
- 3G-ms-init-comb-detach
- 3G-attached
- 2G-attached
- 3G-home-subscribers
- 2G-home-subscribers
- 3G-visiting-national
- 2G-visiting-national
- 3G-visiting-foreign
- 2G-visiting-foreign
- pmm-connected
- pmm-idle
- gprs-standby
- gprs-ready
- 3G-attached-with-pdp

- 2G-attached-with-pdp
- 3G-detached
- 3G-total-attach-req-all
- 3G-total-attach-req
- 3G-total-comb-attach-req
- 2G-total-attach-req-all
- 2G-total-attach-req
- 2G-total-comb-attach-req
- request-requesting-relayed
- request-renewing-relayed
- ack-rx
- ack-for-inform
- ack-renewing-rx
- ack-tx
- ack-renewing-tx
- ack-relayed
- ack-renewing-relayed
- 3G-local-ptmsi-Attch
- 3G-local-ptmsi-Attch-comb
- 3G-remote-ptmsi-Attch
- 3G-remote-ptmsi-Attch-comb
- 2G-local-ptmsi-Attch-comb
- 2G-remote-ptmsi-Attch-comb
- 3G-ret-imsi-attach
- 3G-ret-imsi-attach-comb
- 2G-ret-imsi-attach
- 2G-ret-imsi-attach-comb
- 3G-ret-local-ptmsi-attach
- 3G-ret-local-ptmsi-attach-comb
- 2G-ret-local-ptmsi-attach
- 2G-ret-local-ptmsi-attach-comb
- 3G-ret-remote-ptmsi-attach
- 3G-ret-remote-ptmsi-attach-comb
- 2G-ret-remote-ptmsi-attach
- 2G-ret-remote-ptmsi-attach-comb
- 3G-attach-accept
- 3G-comb-attach-accept
- 3G-ret-attach-accept

- 3G-ret-attach-accept-comb
- 2G-ret-attch-accept-comb
- 3G-attach-reject-all
- 3G-attach-reject
- 3G-attach-reject-comb
- 2G-attach-reject-all
- 2G-attach-reject
- 2G-attach-reject-comb
- 3G-comb-attach-rej-imsi-unknown-at-hlr
- 2G-comb-attach-rej-imsi-unknown-at-hlr
- 3G-comb-attach-rej-illegal-ms
- 2G-comb-attach-rej-illegal-ms
- 3G-comb-attach-rej-illegal-me
- 2G-comb-attach-rej-illegal-me
- 3G-comb-gprs-service-not-allowed
- 2G-comb-gprs-service-not-allowed
- 3G-comb-gprs-and-non-gprs-svc-not-allow
- 2G-comb-gprs-and-non-gprs-svc-not-allow
- 3G-comb-attach-rej-msid-not-derived-by-nwt
- 2G-comb-attach-rej-msid-not-derived-by-nwt
- 3G-comb-attach-rej-implicitly-detach
- 2G-comb-attach-rej-implicitly-detach
- 3G-comb-attach-rej-plmn-not-allowed
- 2G-comb-attach-rej-plmn-not-allowed
- 3G-comb-attach-rej-la-not-allowed
- 2G-comb-attach-rej-la-not-allowed
- 3G-comb-roam-not-allow-in-loc-area
- 2G-comb-roam-not-allow-in-loc-area
- 3G-comb-gprs-svc-not-allow-in-plmn
- 2G-comb-gprs-svc-not-allow-in-plmn
- 3G-comb-no-suitable-cells-in-loc-area
- 2G-comb-no-suitable-cells-in-loc-area
- 3G-comb-attach-rej-msc-not-reachable
- 2G-comb-attach-rej-msc-not-reachable
- 3G-comb-attach-rej-network-failure
- 2G-comb-attach-rej-network-failure
- 3G-comb-attach-rej-mac-failure
- 2G-comb-attach-rej-mac-failure

- 3G-comb-attach-rej-sync-failure
- 2G-comb-attach-rej-sync-failure
- 3G-comb-attach-rej-congestion
- 2G-comb-attach-rej-congestion
- 3G-comb-attach-rej-gsm-auth-unacceptable
- 2G-comb-attach-rej-gsm-auth-unacceptable
- 3G-comb-attach-rej-no-pdp-ctx-activated
- 2G-comb-attach-rej-no-pdp-ctx-activated
- 3G-comb-attach-rej-retry-from-new-cell
- 2G-comb-attach-rej-retry-from-new-cell
- 3G-comb-attach-rej-sem-wrong-msg
- 2G-comb-attach-rej-sem-wrong-msg
- 3G-comb-attach-rej-invalid-mand-info
- 2G-comb-attach-rej-invalid-mand-info
- 3G-comb-attach-rej-msg-type-not-exist
- 2G-comb-attach-rej-msg-type-not-exist
- 3G-comb-attach-rej-msg-type-not-comp-pstate
- 2G-comb-attach-rej-msg-type-not-comp-pstate
- 3G-comb-attach-rej-ie-non-existent
- 2G-comb-attach-rej-ie-non-existent
- 3G-comb-attach-rej-conditional-ie-err
- 2G-comb-attach-rej-conditional-ie-err
- 3G-comb-attach-rej-msg-not-comp-prot-state
- 2G-comb-attach-rej-msg-not-comp-prot-state
- 3G-comb-attach-rej-protocol-error
- 2G-comb-attach-rej-protocol-error
- 3G-comb-attach-rej-unknown-cause
- 2G-comb-attach-rej-unknown-cause
- 3G-total-attach-fail
- 3G-total-attach-fail-comb
- 2G-total-attach-fail
- 2G-total-attach-fail-comb
- 3G-attach-fail-Iu_release-comb
- 3G-attach-fail-ongoing-proc-comb
- 2G-attach-fail-ongoing-proc-comb
- 3G-comb-rau-reject
- 3G-comb-inter-rau-reject
- 2G-comb-rau-reject

- 2G-comb-inter-rau-reject
- 3G-comb-rau-rej-imsi-unknown-hlr
- 2G-comb-rau-rej-imsi-unknown-hlr
- 3G-comb-rau-rej-illegal-ms
- 2G-comb-rau-rej-illegal-ms
- 3G-comb-rau-rej-illegal-me
- 2G-comb-rau-rej-illegal-me
- 3G-comb-rau-rej-gprs-svc-not-allow
- 2G-comb-rau-rej-gprs-svc-not-allow
- 3G-comb-rau-rej-nongprs-svc-not-allow
- 2G-comb-rau-rej-nongprs-svc-not-allow
- 3G-comb-rau-rej-msid-not-derived-by-nw
- 2G-comb-rau-rej-msid-not-derived-by-nw
- 3G-comb-rau-rej-implicitly-detach
- 2G-comb-rau-rej-implicitly-detach
- 3G-comb-rau-rej-plmn-not-allowed
- 3G-comb-rau-rej-loc-area-not-allowed
- 2G-comb-rau-rej-loc-area-not-allowed
- 3G-comb-rau-rej-roam-not-allowed-larea
- 2G-comb-rau-rej-roam-not-allowed-larea
- 3G-comb-rau-rej-gprs-svc-not-allowed-plmn
- 2G-comb-rau-rej-gprs-svc-not-allowed-plmn
- 3G-comb-rau-rej-congestion
- 2G-comb-rau-rej-congestion
- 3G-comb-rau-rej-gsm-auth-unacceptable
- 2G-comb-rau-rej-gsm-auth-unacceptable
- 3G-comb-rau-rej-no-pdp-ctx-actv
- 2G-comb-rau-rej-no-pdp-ctx-actv
- 3G-comb-rau-rej-retry-from-new-cell
- 2G-comb-rau-rej-retry-from-new-cell
- 3G-comb-rau-rej-sem-wrong-msg
- 2G-comb-rau-rej-sem-wrong-msg
- 3G-comb-rau-rej-inval-mand-info
- 2G-comb-rau-rej-inval-mand-info
- 3G-comb-rau-rej-msg-type-non-exist
- 2G-comb-rau-rej-msg-type-non-exist
- 3G-comb-rau-rej-mtype-incompat-pstate
- 2G-comb-rau-rej-mtype-incompat-pstate

- 3G-comb-rau-rej-ie-non-existent
- 2G-comb-rau-rej-ie-non-existent
- 3G-comb-rau-rej-cond-ie-error
- 2G-comb-rau-rej-cond-ie-error
- 3G-comb-rau-rej-msg-incompat-pstate
- 2G-comb-rau-rej-msg-incompat-pstate
- 3G-comb-rau-rej-prot-error
- 2G-comb-rau-rej-prot-error
- 3G-comb-rau-rej-unknown-error
- 2G-comb-rau-rej-unknown-error
- 3G-comb-irau-rej-imsi-unknown-hlr
- 2G-comb-irau-rej-imsi-unknown-hlr
- 3G-comb-irau-rej-illegal-ms
- 2G-comb-irau-rej-illegal-ms
- 3G-comb-irau-rej-illegal-me
- 2G-comb-irau-rej-illegal-me
- 3G-comb-irau-rej-gprs-svc-not-allow
- 2G-comb-irau-rej-gprs-svc-not-allow
- 3G-comb-irau-rej-nongprs-svc-not-allow
- 2G-comb-irau-rej-nongprs-svc-not-allow
- 3G-comb-irau-rej-msid-not-derived-by-nw
- 2G-comb-irau-rej-msid-not-derived-by-nw
- 3G-comb-irau-rej-implicitly-detach
- 2G-comb-irau-rej-implicitly-detach
- 3G-comb-irau-rej-plmn-not-allowed
- 3G-comb-irau-rej-loc-area-not-allowed
- 2G-comb-irau-rej-loc-area-not-allowed
- 3G-comb-irau-rej-roam-not-allowed-larea
- 2G-comb-irau-rej-roam-not-allowed-larea
- 3G-comb-irau-rej-gprs-svc-not-allowed-plmn
- 2G-comb-irau-rej-gprs-svc-not-allowed-plmn
- 3G-comb-irau-rej-no-cells-in-location-area
- 2G-comb-irau-rej-no-cells-in-location-area
- 3G-comb-irau-rej-msc-not-reachable
- 2G-comb-irau-rej-msc-not-reachable
- 3G-comb-irau-rej-network-failure
- 2G-comb-irau-rej-network-failure
- 3G-comb-irau-rej-mac-failure

- 2G-comb-irau-rej-mac-failure
- 3G-comb-irau-rej-syn-failure
- 2G-comb-irau-rej-syn-failure
- 3G-comb-irau-rej-congestion
- 2G-comb-irau-rej-congestion
- 3G-comb-irau-rej-gsm-auth-unacceptable
- 2G-comb-irau-rej-gsm-auth-unacceptable
- 3G-comb-irau-rej-no-pdp-ctx-actv
- 2G-comb-irau-rej-no-pdp-ctx-actv
- 3G-comb-irau-rej-retry-from-new-cell
- 2G-comb-irau-rej-retry-from-new-cell
- 3G-comb-irau-rej-sem-wrong-msg
- 2G-comb-irau-rej-sem-wrong-msg
- 3G-comb-irau-rej-inval-mand-info
- 2G-comb-irau-rej-inval-mand-info
- 3G-comb-irau-rej-msg-type-non-exist
- 2G-comb-irau-rej-msg-type-non-exist
- 3G-comb-irau-rej-mtype-incompat-pstate
- 2G-comb-irau-rej-mtype-incompat-pstate
- 3G-comb-irau-rej-ie-non-existent
- 2G-comb-irau-rej-ie-non-existent
- 3G-comb-irau-rej-cond-ie-error
- 2G-comb-irau-rej-cond-ie-error
- 3G-comb-irau-rej-msg-not-compat-pstate
- 2G-comb-irau-rej-msg-not-compat-pstate
- 3G-comb-irau-rej-prot-error
- 2G-comb-irau-rej-prot-error
- 3G-comb-irau-rej-unknown-error
- 2G-comb-irau-rej-unknown-error
- 3G-total-intra-rau-failure-comb
- 2G-total-comb-inter-rau-failure
- 3G-paging-request
- 2G-paging-request
- 3G-ret-paging-request
- 2G-ret-pagin-request
- 3G-paging-success
- 3G-cs-page-request
- 2G-cs-page-request

- 3G-cs-page-response
- 2G-cs-page-response
- 3G-tmsi-identity-request
- 2G-tmsi-identity-request
- 3G-ret-tmsi-identity-request
- 2G-ret-tmsi-identity-request
- 3G-tmsi-identity-response
- 2G-tmsi-identity-response
- 2G-ready-timer-expiry
- 3G-total-num-actv-pdp
- 2G-total-num-actv-pdp
- 3G-total-actv-pdp-with-dir-tunnel
- 3G-actv-rej-service-not-subscribed
- 2G-actv-rej-service-not-subscribed
- 3G-sec-actv-rej-odb
- 2G-sec-actv-rej-odb
- 3G-sec-actv-rej-insufficient-resources
- 2G-sec-actv-rej-insufficient-resources
- 3G-sec-actv-rej-by-ggsn
- 2G-sec-actv-rej-by-ggsn
- 3G-sec-actv-rej-unspecified-error
- 2G-sec-actv-rej-unspecified-error
- 3G-sec-actv-rej-service-not-supported
- 2G-sec-actv-rej-service-not-supported
- 3G-sec-actv-rej-service-not-subscribed
- 2G-sec-actv-rej-service-not-subscribed
- 3G-sec-actv-rej-svc-opt-tmp-out-of-order
- 2G-sec-actv-rej-svc-opt-tmp-out-of-order
- 3G-sec-actv-rej-semantically-incorrect
- 2G-sec-actv-rej-semantically-incorrect
- 3G-sec-actv-rej-invalid-mandatory-info
- 2G-sec-actv-rej-invalid-mandatory-info
- 3G-sec-actv-rej-msg-type-non-existent
- 2G-sec-actv-rej-msg-type-non-existent
- 3G-sec-actv-rej-ie-non-existent
- 2G-sec-actv-rej-ie-non-existent
- 3G-sec-actv-rej-conditional-ie-err
- 2G-sec-actv-rej-conditional-ie-err

- 3G-sec-actv-rej-msg-not-compat-prot-state
- 2G-sec-actv-rej-msg-not-compat-prot-state
- 3G-sec-actv-rej-recovery-on-timer-expiry
- 2G-sec-actv-rej-recovery-on-timer-expiry
- 3G-sec-actv-rej-prot-err-unspecified
- 2G-sec-actv-rej-prot-err-unspecified
- 3G-sec-actv-rej-semantic-error-tft-operation
- 2G-sec-actv-rej-semantic-error-tft-operation
- 3G-sec-actv-rej-syntax-err-in-tft-operation
- 2G-sec-actv-rej-syntax-err-in-tft-operation
- 3G-sec-actv-rej-unknown-pdp-context
- 2G-sec-actv-rej-unknown-pdp-context
- 3G-sec-actv-rej-semantic-err-in-pkt-filter
- 2G-sec-actv-rej-semantic-err-in-pkt-filter
- 3G-sec-actv-rej-syntax-err-in-pkt-filter
- 2G-sec-actv-rej-syntax-err-in-pkt-filter
- 3G-sec-actv-rej-pdp-notft-actv
- 2G-sec-actv-rej-pdp-notft-actv
- 3G-ms-modify-rej-insufficient-resources
- 2G-ms-modify-rej-insufficient-resources
- 3G-ms-modify-rej-service-opt-not-supported
- 2G-ms-modify-rej-service-opt-not-supported
- 3G-ms-modify-rej-semantic-err-tft-operation
- 2G-ms-modify-rej-semantic-err-tft-operation
- 3G-ms-modify-rej-syntax-err-tft-operation
- 2G-ms-modify-rej-syntax-err-tft-operation
- 3G-ms-modify-rej-semnatic-err-pkt-filter
- 2G-ms-modify-rej-semnatic-err-pkt-filter
- 3G-ms-modify-rej-syntax-err-pkt-filter
- 2G-ms-modify-rej-syntax-err-pkt-filter
- 3G-ms-modify-rej-semnatic-incorrect-message
- 2G-ms-modify-rej-semnatic-incorrect-message
- 3G-ms-modify-rej-invalid-mand-info
- 2G-ms-modify-rej-invalid-mand-info
- 3G-ms-modify-rej-ie-non-existent
- 2G-ms-modify-rej-ie-non-existent
- 3G-ms-modify-rej-conditional-ie-err
- 2G-ms-modify-rej-conditional-ie-err

- 3G-ms-modify-rej-msg-not-compatible-prot-state
- 2G-ms-modify-rej-msg-not-compatible-prot-state
- 3G-ms-modify-rej-rcvry-on-tmr-expiry
- 2G-ms-modify-rej-rcvry-on-tmr-expiry
- 3G-ms-modify-rej-prot-err-unspec
- 2G-ms-modify-rej-prot-err-unspec
- srns-ctx-deny-no-response-from-rnc
- map-mo-fwd-req-sent
- map-mo-fwd-rsp-rcvd
- map-mo-fwd-rsp-failed
- map-mo-fwd-rsp-time-out
- map-mt-fwd-req-sent
- map-mt-fwd-rsp-rcvd
- map-mt-fwd-rsp-failed
- map-ready-for-sm-req
- map-ready-for-sm-rsp
- map-ready-for-sm-rsp-failed
- map-ready-for-sm-rsp-time-out
- tcap-total-active-trans
- tcap-total-active-invoks
- mo-sms-in-progress
- mt-sms-in-progress
- sms-memory-available-in-progress
- mo-sms-attempted
- mo-sms-successful
- mt-sms-attempted
- mt-sms-successful
- sms-memory-available-attempted
- sms-memory-available-successful
- conn-prot-data-tx
- conn-prot-data-rx
- conn-prot-ack-tx
- conn-prot-ack-rx
- conn-prot-error-tx
- conn-prot-error-rx
- conn-prot-error-nwt-fail-tx
- conn-prot-error-nwt-fail-rx
- conn-prot-error-congestion-tx

- conn-prot-error-congestion-rx
- conn-prot-error-invalid-tid-tx
- conn-prot-error-invalid-tid-rx
- conn-prot-error-invalid-semantic-tx
- conn-prot-error-invalid-semantic-rx
- conn-prot-error-invalid-mand-info-tx
- conn-prot-error-invalid-mand-info-rx
- conn-prot-error-invalid-msg-type-tx
- conn-prot-error-invalid-msg-type-rx
- conn-prot-error-invalid-prot-state-tx
- conn-prot-error-invalid-prot-state-rx
- conn-prot-error-invalid-ie-tx
- conn-prot-error-invalid-ie-rx
- conn-prot-error-protocol-error-tx
- conn-prot-error-protocol-error-rx
- conn-prot-error-undefined-cause-tx
- conn-prot-error-undefined-cause-rx
- conn-prot-data-dropped
- conn-prot-ack-dropped
- conn-prot-error-dropped
- conn-prot-inval-tid-rcvd
- relay-prot-data-tx
- relay-prot-data-rx
- relay-prot-ack-tx
- relay-prot-ack-rx
- relay-prot-err-tx
- relay-prot-err-rx
- relay-prot-err-unassigned-num
- relay-prot-err-opr-determ-barring
- relay-prot-err-call-barred
- relay-prot-err-reserved
- relay-prot-err-sm-transfer-rej
- relay-prot-err-dest-out-of-order
- relay-prot-err-unidentified-subs
- relay-prot-err-facility-rej
- relay-prot-err-unknown-subs
- relay-prot-err-netwk-out-of-order
- relay-prot-err-temp-fail

- relay-prot-err-congestion
- relay-prot-err-not-subscribed
- relay-prot-err-not-implemented
- relay-prot-err-interworking-err
- relay-prot-err-res-unavail
- relay-prot-err-mem-capacity-exceed
- relay-prot-err-inval-ref-num-tx
- relay-prot-err-inval-ref-num-rx
- relay-prot-err-inval-semantic-tx
- relay-prot-err-inval-semantic-rx
- relay-prot-err-inval-mand-info-tx
- relay-prot-err-inval-mand-info-rx
- relay-prot-err-inval-msg-type-tx
- relay-prot-err-inval-msg-type-rx
- relay-prot-err-inval-prot-state-tx
- relay-prot-err-inval-prot-state-rx
- relay-prot-err-inval-ie-tx
- relay-prot-err-inval-ie-rx
- relay-prot-err-protocol-error-tx
- relay-prot-err-unidentified-error-tx
- relay-prot-err-unidentified-error-rx
- relay-prot-data-dropped
- relay-prot-ack-dropped
- relay-prot-error-dropped
- relay-prot-decode-failure
- concat-mo-sms
- conn-prot-timer-expiry
- tr1n-timer-expiry
- tr2n-timer-expiry
- conn-prot-data-retrans
- relay-prot-msg-encode-fail
- conn-prot-data-tx-fail
- conn-prot-data-inval-tid
- conn-prot-max-retrans-reached
- mt-fail-no-db-rec
- mt-fail-conn-prot-data-no-ack-rcvd
- mt-fail-fwd-busy-subs
- mt-fail-fwd-detached-subs

- mt-fail-mt-queue-full
- 3G-comb-rau-rej-no-cells-in-loc-area
- 2G-comb-rau-rej-no-cells-in-loc-area
- 3G-comb-rau-rej-msc-not-reachable
- 2G-comb-rau-rej-msc-not-reachable
- 3G-comb-rau-rej-network-failure
- 2G-comb-rau-rej-network-failure
- 3G-comb-rau-rej-mac-failure
- 2G-comb-rau-rej-mac-failure
- 3G-comb-rau-rej-syn-failure
- 2G-comb-rau-rej-syn-failure
- 3G-actv-fail-iu-release-before-activate
- 3G-actv-fail-gaurd-timer-expiry 3
- G-actv-fail-duplicate-activation
- 3G-actv-fail-other-ongoing-procedure
- 3G-actv-fail-tunnel-deactivation
- 3G-actv-fail-handoff-before-activate-over
- 3G-actv-fail-detach-before-activate-over
- 3G-actv-fail-invalid-message-content
- 2G-actv-fail-gaurd-timer-expiry
- 2G-actv-fail-duplicate-activation
- 2G-actv-fail-other-ongoing-procedure
- 2G-actv-fail-tunnel-deactivation
- 2G-actv-fail-handoff-before-activate-over
- 2G-actv-fail-detach-before-activate-over
- 2G-actv-fail-invalid-msg-content
- inter-system-2G-to-3G-rau-requests
- inter-system-2G-to-3G-rau-accepts
- inter-system-2G-to-3G-comb-rau-requests inter-system-2G-to-3G-comb-rau-accepts
- inter-system-2G-to-3G-rau-rejects
- inter-system-2G-to-3G-comb-rau-rejects
- inter-system-2G-to-3G-attach-requests
- inter-system-2G-to-3G-attach-accepts
- inter-system-2G-to-3G-attach-rejects
- inter-system-2G-to-3G-comb-attach-requests
- inter-system-2G-to-3G-comb-attach-accepts
- inter-system-2G-to-3G-comb-attach-rejects
- inter-system-3G-to-2G-rau-requests

- inter-system-3G-to-2G-rau-accepts
- inter-system-3G-to-2G-comb-rau-requests
- inter-system-3G-to-2G-comb-rau-accepts
- inter-system-3G-to-2G-rau-rejects
- inter-system-3G-to-2G-comb-rau-rejects
- inter-system-3G-to-2G-attach-requests
- inter-system-3G-to-2G-attach-accepts
- inter-system-3G-to-2G-attach-rejects
- inter-system-3G-to-2G-comb-attach-requests
- inter-system-3G-to-2G-comb-attach-accepts
- inter-system-3G-to-2G-comb-attach-rejects
- 2G-intra-prau-rej-msc-not-reachable
- 3G-intra-prau-rej-network-failure
- 2G-intra-prau-rej-network-failure
- 3G-intra-prau-rej-mac-failure
- 2G-intra-prau-rej-mac-failure
- 3G-intra-prau-rej-syn-failure
- 2G-intra-prau-rej-syn-failure0
- 3G-comb-rau-rej-no-cells-in-loc-area
- 2G-comb-rau-rej-no-cells-in-loc-area
- 3G-comb-rau-rej-msc-not-reachable
- 2G-comb-rau-rej-msc-not-reachable
- 3G-comb-rau-rej-network-failure
- 2G-comb-rau-rej-network-failure
- 3G-comb-rau-rej-mac-failure
- 2G-comb-rau-rej-mac-failure
- 3G-comb-rau-rej-syn-failure
- 2G-comb-rau-rej-syn-failure
- intra-sgsn-inter-system-gsm-to-wcdma-success
- intra-sgsn-inter-system-gsm-to-wcdma-rej
- intra-sgsn-inter-system-gsm-to-wcdma-fail
- intra-sgsn-inter-system-wcdma-to-gsm-success
- intra-sgsn-inter-system-wcdma-to-gsm-rej
- intra-sgsn-inter-system-wcdma-to-gsm-fail
- ps-inter-rat-rau-total
- ps-inter-rat-rau-3g
- ps-inter-rat-rau-2g
- comb-inter-rat-rau-total

- comb-inter-rat-rau-3g
- comb-inter-rat-rau-2g
- ret-ps-inter-rat-rau-total
- ret-ps-inter-rat-rau-3g
- ret-ps-inter-rat-rau-2g
- ret-comb-inter-rat-rau-total
- ret-comb-inter-rat-rau-3g
- ret-comb-inter-rat-rau-2g
- ps-inter-service-rau-total
- ps-inter-service-rau-3g
- ps-inter-service-rau-2g
- comb-inter-service-rau-total
- comb-inter-service-rau-3g
- comb-inter-service-rau-2g
- ret-ps-inter-service-rau-total
- ret-ps-inter-service-rau-3g
- ret-ps-inter-service-rau-2g
- ret-comb-inter-service-rau-total
- ret-comb-inter-service-rau-3g
- ret-comb-inter-service-rau-2g
- ps-inter-rat-rau-acc-total
- ps-inter-rat-rau-acc-3g
- ps-inter-rat-rau-acc-2g
- comb-inter-rat-rau-acc-total
- comb-inter-rat-rau-acc-3g
- comb-inter-rat-rau-acc-2g
- ret-ps-inter-rat-rau-acc-total
- ret-ps-inter-rat-rau-acc-3g
- ret-ps-inter-rat-rau-acc-2g
- ret-comb-inter-rat-rau-acc-total
- ret-comb-inter-rat-rau-acc-3g
- ret-comb-inter-rat-rau-acc-2g
- ps-inter-service-rau-acc-total
- ps-inter-service-rau-acc-3g
- ps-inter-service-rau-acc-2g
- comb-inter-service-rau-acc-total
- comb-inter-service-rau-acc-3g
- comb-inter-service-rau-acc-2g

- ret-ps-inter-service-rau-acc-total
- ret-ps-inter-service-rau-acc-3g
- ret-ps-inter-service-rau-acc-2g
- ret-comb-inter-service-rau-acc-total
- ret-comb-inter-service-rau-acc-3g
- ret-comb-inter-service-rau-acc-2g
- ps-inter-rat-rau-rej-total
- ps-inter-rat-rau-rej-3g
- ps-inter-rat-rau-rej-2g
- comb-inter-rat-rau-rej-total
- comb-inter-rat-rau-rej-3g
- comb-inter-rat-rau-rej-2g
- ps-inter-service-rau-rej-total
- ps-inter-service-rau-rej-3g
- ps-inter-service-rau-rej-2g
- comb-inter-service-rau-rej-total
- comb-inter-service-rau-rej-3g
- comb-inter-service-rau-rej-2g
- 3G-isrv-ps-rej-imsi-unknown-hlr
- 2G-isrv-ps-rej-imsi-unknown-hlr
- 3G-isrv-ps-rej-illegal-ms
- 2G-isrv-ps-rej-illegal-ms
- 3G-isrv-ps-rej-illegal-me
- 2G-isrv-ps-rej-illegal-me
- 3G-isrv-ps-rej-gprs-svc-not-allow
- 2G-isrv-ps-rej-gprs-svc-not-allow
- 3G-isrv-ps-rej-nongprs-svc-not-allow
- 2G-isrv-ps-rej-nongprs-svc-not-allow
- 3G-isrv-ps-rej-msid-not-derived-by-nw
- 2G-isrv-ps-rej-msid-not-derived-by-nw
- 3G-isrv-ps-rej-implicitly-detach
- 2G-isrv-ps-rej-implicitly-detach
- 3G-isrv-ps-rej-plmn-not-allowed
- 2G-isrv-ps-rej-plmn-not-allowed
- 3G-isrv-ps-rej-loc-area-not-allowed
- 2G-isrv-ps-rej-loc-area-not-allowed
- 3G-isrv-ps-rej-roam-not-allowed-larea
- 2G-isrv-ps-rej-roam-not-allowed-larea

- 3G-isrv-ps-rej-gprs-svc-not-allowed-plmn
- 2G-isrv-ps-rej-gprs-svc-not-allowed-plmn
- 3G-isrv-ps-rej-no-cells-in-location-area
- 2G-isrv-ps-rej-no-cells-in-location-area
- 3G-isrv-ps-rej-msc-not-reachable
- 2G-isrv-ps-rej-msc-not-reachable
- 3G-isrv-ps-rej-network-failure
- 2G-isrv-ps-rej-network-failure
- 3G-isrv-ps-rej-mac-failure
- 2G-isrv-ps-rej-mac-failure
- 3G-isrv-ps-rej-syn-failure
- 2G-isrv-ps-rej-syn-failure
- 3G-isrv-ps-rej-congestion
- 2G-isrv-ps-rej-congestion
- 3G-isrv-ps-rej-gsm-auth-unacceptable
- 2G-isrv-ps-rej-gsm-auth-unacceptable
- 3G-isrv-ps-rej-no-pdp-ctx-actv
- 2G-isrv-ps-rej-no-pdp-ctx-actv
- 3G-isrv-ps-rej-retry-from-new-cell
- 2G-isrv-ps-rej-retry-from-new-cell
- 3G-isrv-ps-rej-sem-wrong-msg
- 2G-isrv-ps-rej-sem-wrong-msg
- 3G-isrv-ps-rej-inval-mand-info
- 2G-isrv-ps-rej-inval-mand-info
- 3G-isrv-ps-rej-msg-type-non-exist
- 2G-isrv-ps-rej-msg-type-non-exist
- 3G-isrv-ps-rej-mtype-incompat-pstate
- 2G-isrv-ps-rej-mtype-incompat-pstate
- 3G-isrv-ps-rej-ie-non-existent
- 2G-isrv-ps-rej-ie-non-existent
- 3G-isrv-ps-rej-cond-ie-error
- 2G-isrv-ps-rej-cond-ie-error
- 3G-isrv-ps-rej-msg-not-compat-pstate
- 2G-isrv-ps-rej-msg-not-compat-pstate
- 3G-isrv-ps-rej-prot-error
- 2G-isrv-ps-rej-prot-error
- 3G-isrv-ps-rej-unknown-error
- 2G-isrv-ps-rej-unknown-error

- 3G-isrv-comb-rej-imsi-unknown-hlr
- 2G-isrv-comb-rej-imsi-unknown-hlr
- 3G-isrv-comb-rej-illegal-ms
- 2G-isrv-comb-rej-illegal-ms
- 3G-isrv-comb-rej-illegal-me
- 2G-isrv-comb-rej-illegal-me
- 3G-isrv-comb-rej-gprs-svc-not-allow
- 2G-isrv-comb-rej-gprs-svc-not-allow
- 3G-isrv-comb-rej-nongprs-svc-not-allow
- 2G-isrv-comb-rej-nongprs-svc-not-allow
- 3G-isrv-comb-rej-msid-not-derived-by-nw
- 2G-isrv-comb-rej-msid-not-derived-by-nw
- 3G-isrv-comb-rej-implicitly-detach
- 2G-isrv-comb-rej-implicitly-detach
- 3G-isrv-comb-rej-plmn-not-allowed
- 2G-isrv-comb-rej-plmn-not-allowed
- 3G-isrv-comb-rej-loc-area-not-allowed
- 2G-isrv-comb-rej-loc-area-not-allowed
- 3G-isrv-comb-rej-roam-not-allowed-larea
- 2G-isrv-comb-rej-roam-not-allowed-larea
- 3G-isrv-comb-rej-gprs-svc-not-allowed-plmn
- 2G-isrv-comb-rej-gprs-svc-not-allowed-plmn
- 3G-isrv-comb-rej-no-cells-in-location-area
- 2G-isrv-comb-rej-no-cells-in-location-area
- 3G-isrv-comb-rej-msc-not-reachable
- 2G-isrv-comb-rej-msc-not-reachable
- 3G-isrv-comb-rej-network-failure
- 2G-isrv-comb-rej-network-failure
- 3G-isrv-comb-rej-mac-failure
- 2G-isrv-comb-rej-mac-failure
- 3G-isrv-comb-rej-syn-failure
- 2G-isrv-comb-rej-syn-failure
- 3G-isrv-comb-rej-congestion
- 2G-isrv-comb-rej-congestion
- 3G-isrv-comb-rej-gsm-auth-unacceptable
- 2G-isrv-comb-rej-gsm-auth-unacceptable
- 3G-isrv-comb-rej-no-pdp-ctx-actv
- 2G-isrv-comb-rej-no-pdp-ctx-actv

- 3G-isrv-comb-rej-retry-from-new-cell
- 2G-isrv-comb-rej-retry-from-new-cell
- 3G-isrv-comb-rej-sem-wrong-msg
- 2G-isrv-comb-rej-sem-wrong-msg
- 3G-isrv-comb-rej-inval-mand-info
- 2G-isrv-comb-rej-inval-mand-info
- 3G-isrv-comb-rej-msg-type-non-exist
- 2G-isrv-comb-rej-msg-type-non-exist
- 3G-isrv-comb-rej-mtype-incompat-pstate
- 2G-isrv-comb-rej-mtype-incompat-pstate
- 3G-isrv-comb-rej-ie-non-existent
- 2G-isrv-comb-rej-ie-non-existent
- 3G-isrv-comb-rej-cond-ie-error
- 2G-isrv-comb-rej-cond-ie-error
- 3G-isrv-comb-rej-msg-not-compat-pstate
- 2G-isrv-comb-rej-msg-not-compat-pstate
- 3G-isrv-comb-rej-prot-error
- 2G-isrv-comb-rej-prot-error
- 3G-isrv-comb-rej-unknown-error
- 2G-isrv-comb-rej-unknown-error
- 3G-irat-ps-rej-imsi-unknown-hlr
- 2G-irat-ps-rej-imsi-unknown-hlr
- 3G-irat-ps-rej-illegal-ms
- 2G-irat-ps-rej-illegal-ms
- 3G-irat-ps-rej-illegal-me
- 2G-irat-ps-rej-illegal-me
- 3G-irat-ps-rej-gprs-svc-not-allow
- 2G-irat-ps-rej-gprs-svc-not-allow
- 3G-irat-ps-rej-nongprs-svc-not-allow
- 2G-irat-ps-rej-nongprs-svc-not-allow
- 3G-irat-ps-rej-msid-not-derived-by-nw
- 2G-irat-ps-rej-msid-not-derived-by-nw
- 3G-irat-ps-rej-implicitly-detach
- 2G-irat-ps-rej-implicitly-detach
- 3G-irat-ps-rej-plmn-not-allowed
- 2G-irat-ps-rej-plmn-not-allowed
- 3G-irat-ps-rej-loc-area-not-allowed
- 2G-irat-ps-rej-loc-area-not-allowed

- 3G-irat-ps-rej-roam-not-allowed-larea
- 2G-irat-ps-rej-roam-not-allowed-larea
- 3G-irat-ps-rej-gprs-svc-not-allowed-plmn
- 2G-irat-ps-rej-gprs-svc-not-allowed-plmn
- 3G-irat-ps-rej-no-cells-in-location-area
- 2G-irat-ps-rej-no-cells-in-location-area
- 3G-irat-ps-rej-msc-not-reachable
- 2G-irat-ps-rej-msc-not-reachable
- 3G-irat-ps-rej-network-failure
- 2G-irat-ps-rej-network-failure
- 3G-irat-ps-rej-mac-failure
- 2G-irat-ps-rej-mac-failure
- 3G-irat-ps-rej-syn-failure
- 2G-irat-ps-rej-syn-failure
- 3G-irat-ps-rej-congestion
- 2G-irat-ps-rej-congestion
- 3G-irat-ps-rej-gsm-auth-unacceptable
- 2G-irat-ps-rej-gsm-auth-unacceptable
- 3G-irat-ps-rej-no-pdp-ctx-actv
- 2G-irat-ps-rej-no-pdp-ctx-actv
- 3G-irat-ps-rej-retry-from-new-cell
- 2G-irat-ps-rej-retry-from-new-cell
- 3G-irat-ps-rej-sem-wrong-msg
- 2G-irat-ps-rej-sem-wrong-msg
- 3G-irat-ps-rej-inval-mand-info
- 2G-irat-ps-rej-inval-mand-info
- 3G-irat-ps-rej-msg-type-non-exist
- 2G-irat-ps-rej-msg-type-non-exist
- 3G-irat-ps-rej-mtype-incompat-pstate
- 2G-irat-ps-rej-mtype-incompat-pstate
- 3G-irat-ps-rej-ie-non-existent
- 2G-irat-ps-rej-ie-non-existent
- 3G-irat-ps-rej-cond-ie-error
- 2G-irat-ps-rej-cond-ie-error
- 3G-irat-ps-rej-msg-not-compat-pstate
- 2G-irat-ps-rej-msg-not-compat-pstate
- 3G-irat-ps-rej-prot-error
- 2G-irat-ps-rej-prot-error

- 3G-irat-ps-rej-unknown-error
- 2G-irat-ps-rej-unknown-error
- 3G-irat-comb-rej-imsi-unknown-hlr
- 2G-irat-comb-rej-imsi-unknown-hlr
- 3G-irat-comb-rej-illegal-ms
- 2G-irat-comb-rej-illegal-ms
- 3G-irat-comb-rej-illegal-me
- 2G-irat-comb-rej-illegal-me
- 3G-irat-comb-rej-gprs-svc-not-allow
- 2G-irat-comb-rej-gprs-svc-not-allow
- 3G-irat-comb-rej-nongprs-svc-not-allow
- 2G-irat-comb-rej-nongprs-svc-not-allow
- 3G-irat-comb-rej-msid-not-derived-by-nw
- 2G-irat-comb-rej-msid-not-derived-by-nw
- 3G-irat-comb-rej-implicitly-detach
- 2G-irat-comb-rej-implicitly-detach
- 3G-irat-comb-rej-plmn-not-allowed
- 2G-irat-comb-rej-plmn-not-allowed
- 3G-irat-comb-rej-loc-area-not-allowed
- 2G-irat-comb-rej-loc-area-not-allowed
- 3G-irat-comb-rej-roam-not-allowed-larea
- 2G-irat-comb-rej-roam-not-allowed-larea
- 3G-irat-comb-rej-gprs-svc-not-allowed-plmn
- 2G-irat-comb-rej-gprs-svc-not-allowed-plmn
- 3G-irat-comb-rej-no-cells-in-location-area
- 2G-irat-comb-rej-no-cells-in-location-area
- 3G-irat-comb-rej-msc-not-reachable
- 2G-irat-comb-rej-msc-not-reachable
- 3G-irat-comb-rej-network-failure
- 2G-irat-comb-rej-network-failure
- 3G-irat-comb-rej-mac-failure
- 2G-irat-comb-rej-mac-failure
- 3G-irat-comb-rej-syn-failure
- 2G-irat-comb-rej-syn-failure
- 3G-irat-comb-rej-congestion
- 2G-irat-comb-rej-congestion
- 3G-irat-comb-rej-gsm-auth-unacceptable
- 2G-irat-comb-rej-gsm-auth-unacceptable

- 3G-irat-comb-rej-no-pdp-ctx-actv
- 2G-irat-comb-rej-no-pdp-ctx-actv
- 3G-irat-comb-rej-retry-from-new-cell
- 2G-irat-comb-rej-retry-from-new-cell
- 3G-irat-comb-rej-sem-wrong-msg
- 2G-irat-comb-rej-sem-wrong-msg
- 3G-irat-comb-rej-inval-mand-info
- 2G-irat-comb-rej-inval-mand-info
- 3G-irat-comb-rej-msg-type-non-exist
- 2G-irat-comb-rej-msg-type-non-exist
- 3G-irat-comb-rej-mtype-incompat-pstate
- 2G-irat-comb-rej-mtype-incompat-pstate
- 3G-irat-comb-rej-ie-non-existent
- 2G-irat-comb-rej-ie-non-existent
- 3G-irat-comb-rej-cond-ie-error
- 2G-irat-comb-rej-cond-ie-error
- 3G-irat-comb-rej-msg-not-compat-pstate
- 2G-irat-comb-rej-msg-not-compat-pstate
- 3G-irat-comb-rej-prot-error
- 2G-irat-comb-rej-prot-error
- 3G-irat-comb-rej-unknown-error
- 2G-irat-comb-rej-unknown-error
- 2G-sec-actv-rej-qos-not-acc -- This stat is not used and has been deprecated.
- 2G-actv-rej-qos-not-acc -- This stat is not used and has been deprecated.
- 2G-sec-actv-rej-llc-sndcp-fail -- This stat is not used and has been deprecated.
- 2G-actv-rej-llc-sndcp-fail -- This stat is not used and has been deprecated.

sgtp schema

- sgtpc-upc-req-v0-tx
- sgtpc-upc-req-v1-rx
- sgtpc-upc-req-accept-v1-tx
- sgtpc-upc-req-accept-v1-rx
- sgtpc-upc-req-accept-v0-rx
- sgtpc-dpc-req-accept-v1-tx
- sgtpc-dpc-req-accept-v0-tx
- sgtpc-dpc-req-accept-v1-rx
- sgtpc-dpc-req-accept-v0-rx
- sgtpc-total-sri-req
- sgtpc-sri-req-v1

- sgtpc-sri-req-v0
- sgtpc-sri-req-v1-ret
- sgtpc-sri-req-v0-ret
- sgtpc-sri-req-denied
- sgtpc-total-fail-rpt-req
- sgtpc-fail-rpt-req-v1
- sgtpc-fail-rpt-req-v0
- sgtpc-fail-rpt-req-v1-ret
- sgtpc-fail-rpt-req-v0-ret
- sgtpc-fail-rpt-req-denied
- sgtpc-ident-req-accept-v1-tx
- sgtpc-ident-req-accept-v0-tx
- sgtpc-ident-req-accept-v1-rx
- sgtpc-ident-req-accept-v0-rx
- sgtpc-ident-req-denied-tx
- sgtpc-sgsn-ctxt-req-accept-v1-tx
- sgtpc-sgsn-ctxt-req-accept-v0-tx
- sgtpc-sgsn-ctxt-req-accept-v1-rx
- sgtpc-sgsn-ctxt-req-accept-v0-rx
- sgtpc-sgsn-ctxt-ack-accept-v1-tx
- sgtpc-sgsn-ctxt-ack-accept-v0-tx
- sgtpc-sgsn-ctxt-ack-accept-v1-rx
- sgtpc-sgsn-ctxt-ack-accept-v0-rx
- sgtpc-ret-v1-echo-req-rx
- sgtpc-ret-v0-echo-req-rx
- sgtpu-ggsn-pkt-drop-suspend-dealloc-st
- sgtpu-ggsn-byts-drop-suspend-dealloc-st
- sgtpu-rnc-byts-rau-in-active-reg-st
- sgtpu-rnc-pkt-drop-suspended-dealloc-st
- sgtpu-rnc-byts-drop-suspended-dealloc-st
- sgtpu-rnc-pkt-unknown-version
- sgtpu-v1-echo-req-tx
- sgtpu-v0-echo-req-tx
- sgtpu-v1-echo-req-rx
- sgtpu-v0-echo-req-rx
- sgtpu-v1-echo-rsp-tx
- sgtpu-v0-echo-rsp-tx
- sgtpu-v1-echo-rsp-rx

- sgtpu-v0-echo-rsp-rx
- sgtpu-v1-echo-req-retrans
- sgtpu-v0-echo-req-retrans
- sgtpu-sgsn-unsolicited-data-pkt
- sgtpu-sgsn-err-ind-for-unsolicited-pkt
- sgtpu-total-active-ggsn
- sgtpu-total-active-rnc
- sgtpu-ggsn-pkt-iu-release
- sgtpu-ggsn-byts-iu-release
- sgtpu-ggsn-pkt-t3-tmr-expiry
- sgtpu-ggsn-byts-t3-tmr-expiry
- sgtpu-ggsn-pkt-forwarded
- sgtpu-ggsn-byts-forwarded
- sgtpu-ggsn-pkt-bvc-block
- sgtpu-ggsn-byts-bvc-block
- sgtpc-upc-req-accept-tx
- sgtpc-upc-req-accept-rx
- sgtpc-dpc-req-accept-tx
- sgtpc-dpc-req-accept-rx
- sgtpc-ident-req-accept-tx
- sgtpc-ident-req-accept-rx
- sgtpc-sgsn-ctxt-req-accept-tx
- sgtpc-sgsn-ctxt-req-accept-rx
- sgtpc-sgsn-ctxt-ack-accept-tx
- sgtpc-sgsn-ctxt-ack-accept-rx
- sgtpu-echo-req-tx
- sgtpu-echo-req-rx
- sgtpu-echo-rsp-tx
- sgtpu-echo-rsp-rx

ss7link schema

The following are new for Release 8.0:

- ss7-link-qsaal-recovery-ack-tx

The following are new for Release 8.1

- ss7-link-mtp3-inhibited-duration

ss7rd schema

- ss7rd-sctp-init-ack-tx
- ss7rd-sctp-init-ack-rx

- ss7rd-sctp-shutdown-ack-tx
- ss7rd-sctp-heartbeat-ack-rx
- ss7rd-m3ua-scon-tx
- ss7rd-m3ua-deregrsp-tx
- ss7rd-m3ua-duna-rx
- ss7rd-m3ua-scon-rx
- ss7rd-m3ua-deregrsp-rx
- ss7rd-m3ua-psp-scon-tx
- ss7rd-m3ua-psp-deregrsp-tx
- ss7rd-m3ua-psp-duna-rx
- ss7rd-m3ua-psp-scon-rx
- ss7rd-m3ua-psp-deregrsp-rx
- ss7rd-m3ua-psp-congestion-level1

system schema

The following are new for Release 8.0:

- cf-cache-flushes
- cf-cache-has-path-hits
- cf-cache-hits
- cf-cache-misses
- cf-cat-abor-pkts-hit
- cf-cat-abor-pkts-block
- cf-cat-adult-pkts-hit
- cf-cat-adult-pkts-block
- cf-cat-adv-pkts-hit
- cf-cat-adv-pkts-block
- cf-cat-advert-pkts-hit
- cf-cat-advert-pkts-block
- cf-cat-anon-pkts-hit
- cf-cat-anon-pkts-block
- cf-cat-art-pkts-hit
- cf-cat-art-pkts-block
- cf-cat-auct-pkts-hit
- cf-cat-auct-pkts-block
- cf-cat-auto-pkts-hit
- cf-cat-auto-pkts-block
- cf-cat-black-pkts-hit
- cf-cat-black-pkts-block
- cf-cat-blog-pkts-hit

- cf-cat-blog-pkts-block
- cf-cat-busi-pkts-hit
- cf-cat-busi-pkts-block
- cf-cat-car-pkts-hit
- cf-cat-car-pkts-block
- cf-cat-chat-pkts-hit
- cf-cat-chat-pkts-block
- cf-cat-clean-pkts-hit
- cf-cat-clean-pkts-block
- cf-cat-cmc-pkts-hit
- cf-cat-cmc-pkts-block
- cf-cat-cporn-pkts-hit
- cf-cat-cporn-pkts-block
- cf-cat-crime-pkts-hit
- cf-cat-crime-pkts-block
- cf-cat-cult-pkts-hit
- cf-cat-cult-pkts-block
- cf-cat-drug-pkts-hit
- cf-cat-drug-pkts-block
- cf-cat-dynam-pkts-hit
- cf-cat-dynam-pkts-block
- cf-cat-edu-pkts-hit
- cf-cat-edu-pkts-block
- cf-cat-ent-pkts-hit
- cf-cat-ent-pkts-block
- cf-cat-esrb-pkts-hit
- cf-cat-esrb-pkts-block
- cf-cat-fin-pkts-hit
- cf-cat-fin-pkts-block
- cf-cat-forum-pkts-hit
- cf-cat-forum-pkts-block
- cf-cat-gamb-pkts-hit
- cf-cat-gamb-pkts-block
- cf-cat-game-pkts-hit
- cf-cat-game-pkts-block
- cf-cat-glam-pkts-hit
- cf-cat-glam-pkts-block
- cf-cat-govern-pkts-hit

- cf-cat-govern-pkts-block
- cf-cat-hack-pkts-hit
- cf-cat-hack-pkts-block
- cf-cat-hate-pkts-hit
- cf-cat-hate-pkts-block
- cf-cat-health-pkts-hit
- cf-cat-health-pkts-block
- cf-cat-hobby-pkts-hit
- cf-cat-hobby-pkts-block
- cf-cat-hosts-pkts-hit
- cf-cat-hosts-pkts-block
- cf-cat-kids-pkts-hit
- cf-cat-kids-pkts-block
- cf-cat-legal-pkts-hit
- cf-cat-legal-pkts-block
- cf-cat-lifes-pkts-hit
- cf-cat-lifes-pkts-block
- cf-cat-mail-pkts-hit
- cf-cat-mail-pkts-block
- cf-cat-mil-pkts-hit
- cf-cat-mil-pkts-block
- cf-cat-news-pkts-hit
- cf-cat-news-pkts-block
- cf-cat-occult-pkts-hit
- cf-cat-occult-pkts-block
- cf-cat-p2p-pkts-hit
- cf-cat-p2p-pkts-block
- cf-cat-peer-pkts-hit
- cf-cat-peer-pkts-block
- cf-cat-pers-pkts-hit
- cf-cat-pers-pkts-block
- cf-cat-phish-pkts-hit
- cf-cat-phish-pkts-block
- cf-cat-poltic-pkts-hit
- cf-cat-poltic-pkts-block
- cf-cat-porn-pkts-hit
- cf-cat-porn-pkts-block
- cf-cat-portal-pkts-hit

- cf-cat-portal-pkts-block
- cf-cat-proxy-pkts-hit
- cf-cat-proxy-pkts-block
- cf-cat-radio-pkts-hit
- cf-cat-radio-pkts-block
- cf-cat-ref-pkts-hit
- cf-cat-ref-pkts-block
- cf-cat-rel-pkts-hit
- cf-cat-rel-pkts-block
- cf-cat-sci-pkts-hit
- cf-cat-sci-pkts-block
- cf-cat-search-pkts-hit
- cf-cat-search-pkts-block
- cf-cat-sftwre-pkts-hit
- cf-cat-sftwre-pkts-block
- cf-cat-shop-pkts-hit
- cf-cat-shop-pkts-block
- cf-cat-sport-pkts-hit
- cf-cat-sport-pkts-block
- cf-cat-spywre-pkts-hit
- cf-cat-spywre-pkts-block
- cf-cat-suic-pkts-hit
- cf-cat-suic-pkts-block
- cf-cat-susp-pkts-hit
- cf-cat-susp-pkts-block
- cf-cat-sxed-pkts-hit
- cf-cat-sxed-pkts-block
- cf-cat-tech-pkts-hit
- cf-cat-tech-pkts-block
- cf-cat-trav-pkts-hit
- cf-cat-trav-pkts-block
- cf-cat-viol-pkts-hit
- cf-cat-viol-pkts-block
- cf-cat-weap-pkts-hit
- cf-cat-weap-pkts-block
- cf-cat-white-pkts-hit
- cf-cat-white-pkts-block
- cf-cat-unknow-pkts-hit

- cf-cat-unknow-pkts-block
- cf-cat-pkts-hit-summary
- cf-cat-pkts-block-summary
- disc-reason-291
- disc-reason-291
- disc-reason-292
- disc-reason-293
- disc-reason-294
- disc-reason-295
- disc-reason-296
- disc-reason-297
- disc-reason-298
- disc-reason-299
- disc-reason-300
- disc-reason-301
- disc-reason-302
- disc-reason-303
- disc-reason-304
- disc-reason-305
- disc-reason-306
- disc-reason-307
- disc-reason-308
- disc-reason-309
- disc-reason-310
- disc-reason-311
- disc-reason-312
- curr-proxy
- curr-relay-agent
- sess-total-setup
- setup-proxy
- setup-relay-agent
- total-released
- rel-proxy-admin-releases
- rel-proxy-bearer-call-term.
- rel-proxy-lease-exp-policy
- rel-proxy-lease-renew-failure
- rel-proxy-ip-mis-match
- rel-proxy-lease-time-mis-match

- rel-proxy-other-reasons
- rel-relay-admin-releases
- rel-relay-bearer-call-ter.
- rel-relay-lease-time-out
- rel-relay-other-reasons
- discover-tx
- discover-retransmitted
- discover-rx
- discover-retried-rx
- discover-relayed
- discoverd-retried-relayed
- offer-rx
- offer-discarded
- offer-tx
- offer-relayed
- request-tx
- request-retransmitted
- request-rx
- request-renewal-rx
- request-requesting-relayed
- request-renewing-relayed
- ack-rx
- ack-for-inform
- ack-renewing-rx
- ack-tx
- ack-renewing-tx
- ack-relayed
- ack-renewing-relayed
- nak-rx
- nak-for-inform
- nak-tx
- nak-relayed
- decline-tx
- decline-rx
- decline-relayed
- release-tx
- release-rx
- release-relayed

- release-for-relay-call
- inform-tx
- inform-retransmitted
- inform-rx
- inform-relayed
- offer-dis-parse-err
- offer-dis-lease-less-than-min
- offer-dis-lease-greater-than-max
- offer-dis-ip-val-failed
- offer-dis-xid-mismatch
- ack-dis-parse-err
- ack-dis-xid-mis-match
- decline-dis-ip-mis-match
- ip-lease-renewal
- failed-ip-lease-renew
- no-reply-from-server
- server-nak
- ip-addr-mis-match
- lease-mis-match

Bulk Statistic Modifications

The following modifications were made for Release 8.0:

Obsoleted Bulk Statistics

None for this release.

gprs schema

- ns-num-bytes-rvcd
- ns-num-bytes-sent
- ns-num-nsvc-failed
- ns-num-nsvc-congest
- ns-num-unit-data-msg-rcvd
- ns-num-unit-data-msg-sent
- ns-num-alive-pdu-rcvd
- ns-num-alive-pdu-sent
- ns-num-alive-ack-pdu-rcvd
- ns-num-alive-ack-pdu-sent
- ns-num-block-pdu-rcvd

- ns-num-block-pdu-sent
- ns-num-block-ack-pdu-rcvd
- ns-num-block-ack-pdu-sent
- ns-num-unblock-pdu-rcvd
- ns-num-unblock-pdu-sent
- ns-num-unblock-ack-pdu-rcvd
- ns-num-unblock-ack-pdu-sent
- ns-num-reset-pdu-rcvd
- ns-num-reset-pdu-sent
- ns-num-reset-ack-pdu-rcvd
- ns-num-reset-ack-pdu-sent
- ns-num-status-pdu-rcvd
- ns-num-status-pdu-sent
- bssgp-radio-status-msg-sent

sgsn schema

- 3G-attached-no-pdp
- 2G-attached-no-pdp
- 3G-rau-rej-imsi-unknown-hlr
- 2G-rau-rej-imsi-unknown-hlr
- 3G-rau-rej-illegal-ms
- 2G-rau-rej-illegal-ms
- 3G-rau-rej-illegal-me
- 2G-rau-rej-illegal-me
- 3G-rau-rej-gprs-svc-not-allow
- 2G-rau-rej-gprs-svc-not-allow
- 3G-rau-rej-gprs-and-nongprs-svc-not-allow
- 2G-rau-rej-gprs-and-nongprs-svc-not-allow
- 3G-rau-rej-msid-not-derived-by-nw
- 2G-rau-rej-msid-not-derived-by-nw
- 3G-rau-rej-implicitly-detach
- 2G-rau-rej-implicitly-detach
- 3G-rau-rej-plmn-not-allowed
- 2G-rau-rej-plmn-not-allowed
- 3G-rau-rej-location-area-not-allowed
- 2G-rau-rej-location-area-not-allowed
- 3G-rau-rej-roam-not-allowed-in-larea
- 2G-rau-rej-roam-not-allowed-in-larea
- 3G-rau-rej-gprs-svc-not-allowed-in-plmn

- 2G-rau-rej-gprs-svc-not-allowed-in-plmn
- 3G-rau-rej-no-cells-in-location-area
- 2G-rau-rej-no-cells-in-location-area
- 3G-rau-rej-msc-not-reachable
- 2G-rau-rej-msc-not-reachable
- 3G-rau-rej-network-failure
- 2G-rau-rej-network-failure
- 3G-rau-rej-mac-failure
- 2G-rau-rej-mac-failure
- 3G-rau-rej-syn-failure
- 2G-rau-rej-syn-failure
- 3G-rau-rej-congestion
- 2G-rau-rej-congestion
- 3G-rau-rej-gsm-auth-unacceptable
- 2G-rau-rej-gsm-auth-unacceptable
- 3G-rau-rej-no-pdp-ctx-actv
- 2G-rau-rej-no-pdp-ctx-actv
- 3G-rau-rej-retry-from-new-cell
- 2G-rau-rej-retry-from-new-cell
- 3G-rau-rej-sem-wrong-msg
- 2G-rau-rej-sem-wrong-msg
- 3G-rau-rej-inval-mand-info
- 2G-rau-rej-inval-mand-info
- 3G-rau-rej-msg-type-non-exist
- 2G-rau-rej-msg-type-non-exist
- 3G-rau-rej-mtype-not-compat-prot-state
- 2G-rau-rej-mtype-not-compat-prot-state
- 3G-rau-rej-ie-non-existent
- 2G-rau-rej-ie-non-existent
- 3G-rau-rej-cond-ie-error
- 2G-rau-rej-cond-ie-error
- 3G-rau-rej-msg-not-compat-prot-state
- 2G-rau-rej-msg-not-compat-prot-state
- 3G-rau-rej-prot-error
- 2G-rau-rej-prot-error
- 3G-rau-rej-unknown-error
- 2G-rau-rej-unknown-error
- 2G-signalling-service-request

- 2G-data-service-request
- 2G-service-response
- 2G-service-reject
- 2G-service-rej-netwk-fail
- 2G-service-rej-imsi-unknown-at-hlr
- 2G-service-rej-msid-not-derived-by-nwtk
- 2G-service-rej-implicity-detach
- 2G-service-rej-illegal-ms
- 2G-service-rej-msg-not-compat-prot-state
- 2G-service-rej-no-pdp-ctx-actv
- 2G-actv-rej-llc-sndcp-fail
- 2G-actv-rej-qos-not-acc
- 3G-actv-rej-semantic-error-tft-operation
- 2G-actv-rej-semantic-error-tft-operation
- 3G-actv-rej-syntax-err-in-tft-operation
- 2G-actv-rej-syntax-err-in-tft-operation
- 3G-actv-rej-unknown-pdp-context
- 2G-actv-rej-unknown-pdp-context
- 3G-actv-rej-semantic-err-in-pkt-filter
- 2G-actv-rej-semantic-err-in-pkt-filter
- 3G-actv-rej-syntax-err-in-pkt-filter
- 2G-actv-rej-syntax-err-in-pkt-filter
- 3G-actv-rej-pdp-notft-actv
- 2G-actv-rej-pdp-notft-actv
- 2G-sec-actv-rej-llc-sndcp-fail
- 2G-sec-actv-rej-qos-not-acc
- rab-assign-rej

sgtp schema

- sgtpc-cpc-req-denied
- sgtpc-upc-req-v0-rx
- sgtpc-fwd-reloc-discard-tx
- sgtpc-fwd-srnsctxt-discard-rx

Web Element Manager Path

Click Accounting | Bulk Statistics Configuration.

Bulk Statistic Enhancements in Release 8.1

This section lists bulk statistic additions and changes in Release 8.1. Detailed information on bulk statistics is located in both the *System Administration Guide* and in the *Statistics and Counters Reference*.

Bulk Statistic Additions

Support for the following bulk statistics has been added:

ECS Schema

The following are new for Release 8.1

- p2p-irc-uplnk-bytes
- p2p-irc-dwlnk-bytes
- p2p-irc-uplnk-pkts
- p2p-irc-dwlnk-pkts
- p2p-steam-uplnk-bytes
- p2p-steam-dwlnk-bytes
- p2p-steam-uplnk-pkts
- p2p-steam-dwlnk-pkts
- p2p-ddlink-uplnk-bytes
- p2p-ddlink-dwlnk-bytes
- p2p-ddlink-uplnk-pkts
- p2p-ddlink-dwlnk-pkts
- p2p-halflife2-uplnk-bytes
- p2p-halflife2-dwlnk-bytes
- p2p-halflife2-uplnk-pkts
- p2p-halflife2-dwlnk-pkts
- p2p-hamachivpn-uplnk-bytes
- p2p-hamachivpn-dwlnk-bytes
- p2p-hamachivpn-uplnk-pkts
- p2p-hamachivpn-dwlnk-pkts
- p2p-tvants-uplnk-bytes
- p2p-tvants-dwlnk-bytes
- p2p-tvants-uplnk-pkts
- p2p-tvants-dwlnk-pkts
- p2p-tvuplayer-uplnk-bytes
- p2p-tvuplayer-dwlnk-bytes
- p2p-tvuplayer-uplnk-pkts
- p2p-tvuplayer-dwlnk-pkts

- p2p-uusee-uplnk-bytes
- p2p-uusee-dwlnk-bytes
- p2p-uusee-uplnk-pkts
- p2p-uusee-dwlnk-pkts
- p2p-vpnx-uplnk-bytes
- p2p-vpnx-dwlnk-bytes
- p2p-vpnx-uplnk-pkts
- p2p-vpnx-dwlnk-pkts
- p2p-vtun-uplnk-bytes
- p2p-vtun-dwlnk-bytes
- p2p-vtun-uplnk-pkts
- p2p-vtun-dwlnk-pkts
- p2p-winmx-uplnk-bytes
- p2p-winmx-dwlnk-bytes
- p2p-winmx-uplnk-pkts
- p2p-winmx-dwlnk-pkts
- p2p-wofwarcraft-uplnk-bytes
- p2p-wofwarcraft-dwlnk-bytes
- p2p-wofwarcraft-uplnk-pkts
- p2p-wofwarcraft-dwlnk-pkts
- p2p-xbox-uplnk-bytes
- p2p-xbox-dwlnk-bytes
- p2p-xbox-uplnk-pkts
- p2p-xbox-dwlnk-pkts

Card Schema

Added following for High Water Peak management counters:

- 15peak-cpubusy
- 5peak-cpubusy
- 15peak-memused
- 5peak-memused
- cpu0-15peak-cpubusy
- cpu0-5peak-cpubusy
- cpu0-15peak-memused
- cpu0-5peak-memused
- cpu1-15peak-cpubusy
- cpu1-5peak-cpubusy
- cpu1-15peak-memused
- cpu1-5peak-memused

- cpu2-15peak-cpubusy
- cpu2-5peak-cpubusy
- cpu2-15peak-memused
- cpu2-5peak-memused
- cpu3-15peak-cpubusy
- cpu3-5peak-cpubusy
- cpu3-15peak-memused
- cpu3-5peak-memused

System Schema

Added following for High Water Peak management counters:

- pdp-ctx-15peak-active
- pdp-ctx-5peak-active

Also added following for bulk statistics enhancement:

- ggsn-ttlsgsnconn
- ggsn-cursgsnact
- sess-ttlcallop
- sess-curaaaacctpending
- sess-total-curr
- hamipv6-totalsubscriber
- curr-proxy
- curr-relay-agent
- dhcp-curservsess
- sess-total-setup
- setup-proxy
- setup-relay-agent
- dhcp-ttlservsess
- total-released
- proxy-bearer-call-term
- proxy-lease-exp-policy
- proxy-lease-renew-failure
- proxy-ip-mis-match
- proxy-lease-time-mis-match
- proxy-other-reasons
- relay-admin-releases
- relay-bearer-call-term
- relay-lease-time-out
- relay-other-reasons

- dhcp-servdisc-admin
- dhcp-servdisc-callterm
- dhcp-servdisc-leasetmo
- dhcp-servdisc-other
- dhcp-msg-discover-tx
- dhcp-msg-discover-retransmitted
- dhcp-msg-discover-rx
- dhcp-msg-discover-retried-rx
- dhcp-msg-discover-relayed
- dhcp-msg-discoverd-retried-relayed
- dhcp-msg-offer-rx
- dhcp-msg-offer-discarded
- dhcp-msg-offer-tx
- dhcp-msg-offer-relayed
- dhcp-msg-request-tx
- dhcp-msg-request-retransmitted
- dhcp-msg-request-rx
- dhcp-msg-request-renewal-rx
- dhcp-msg-request-requesting-relayed
- dhcp-msg-request-renewing-relayed
- dhcp-msg-ack-rx
- dhcp-msg-ack-for-inform
- dhcp-msg-ack-renewing-rx
- dhcp-msg-ack-tx
- dhcp-msg-ack-renewing-tx
- dhcp-msg-ack-relayed
- dhcp-msg-ack-renewing-relayed
- dhcp-msg-nak-rx
- dhcp-msg-nak-for-inform
- dhcp-msg-nak-tx
- dhcp-msg-nak-relayed
- dhcp-msg-decline-tx
- dhcp-msg-decline-rx
- dhcp-msg-decline-relayed
- dhcp-msg-release-tx
- dhcp-msg-release-rx
- dhcp-msg-release-relayed
- dhcp-msg-release-for-relay-call

- dhcp-msg-inform-tx
- dhcp-msg-inform-retransmitted
- dhcp-msg-inform-rx
- dhcp-msg-inform-relayed
- offer-dis-parse-err
- offer-dis-lease-less-than-min
- offer-dis-lease-greater-than-max
- offer-dis-ip-val-failed
- offer-dis-xid-mis-match
- ack-dis-parse-err
- ack-dis-xid-mis-match
- decline-dis-ip-mis-match
- ip-lease-renewal
- failed-ip-lease-renew
- no-reply-from-server
- server-nak
- ip-addr-mis-match
- lease-mis-match
- storage-name
- storage-curavail
- storage-ttlavail
- cf-cat-all-pkts-hit
- cf-cat-all-pkts-block
- cf-cat-timer-pkts-hit
- cf-cat-timer-pkts-block
- cf-cat-xcategory-pkts-hit
- cf-cat-xcategory-pkts-block
- cf-cursub
- cf-ttlsub
- url-blacklisting-hits
- url-blacklisting-misses

Port Schema

Added following for High Water Peak management counters:

- port-5peak-rx-util
- port-5peak-tx-util
- port-15peak-rx-util
- port-15peak-rx-util

GPRS Schema

- packets-sent-to-bsc
- packets-rcvd-from-bsc
- bytes-sent-to-bsc
- bytes-rcvd-from-bsc
- 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

GTPC Schema

Added following for this schema:

- mbms-ses-start-tx- accept
- mbms-ses-start-tx-deny
- mbms-ses-stop-tx
- mbms-ses-stop-tx- accept
- sess-in-preservation-mode
- transition-to-preservation-mode
- transition-to-non-preservation-mode
- sess-in-focs
- cnt-of-release-due-to-other
- cnt-of-release-due-to-violation
- ipca-pdp-context-tx
- ipca-pdp-context-tx-accepted
- ipca-pdp-context-tx-denied
- ipca-reject-rx-no-resources
- ipca-reject-rx-no-mem-avail
- ipca-reject-rx-sys-failure
- ipca-reject-rx-non-existent
- ipca-reject-rx-unsupported-service
- ipca-reject-rx-invalid-msg-format
- ipca-reject-rx-semantic-err-in-tft
- ipca-reject-rx-syntactic-err-in-tft
- ipca-reject-rx-man-ie-incorrect
- ipca-reject-rx-semantic-err-in-pac-filter

- ipca-reject-rx-man-ie-missing
- ipca-reject-rx-optional-ie-incorrect
- ipca-reject-rx-syntactic-err-in-pac-filter
- ipca-reject-rx-ue-not-gprs-rsp
- ipca-reject-rx-ue-refuses
- ipca-reject-rx-invalid-correlation-id

GTPC Schema

Added following for this schema:

- total-gmbcdr-xmit
- total-gmbcdr-rexmit
- total-gmbcdr-accept
- total-gmscdr-fail

System Schema

Added following stats for system setup time counters:

- sess-setuptime-18sec
- sess-setuptime-over18sec

SGSN Schema

Added following stats:

- 3G-actv-fail-phase-2-offload
- 2G-actv-fail-phase-2-offload
- 3G-network-sharing-supp-ue
- 3G-network-sharing-non-supp-ue

CSCF Schema

Added the following stats for this schema:

- de-regs-fromue
- de-regs-fromnw
- reg-resp-4xxrx
- reg-resp-4xxtx
- reg-resp-5xxrx
- reg-resp-5xxtx
- reg-resp-6xxrx
- reg-resp-6xxtx
- rereg-resp-4xxrx
- rereg-resp-4xxtx
- rereg-resp-5xxrx
- rereg-resp-5xxtx

- rereg-resp-6xxrx
- rereg-resp-6xxtx
- dereg-resp-4xxrx
- dereg-resp-4xxtx
- dereg-resp-5xxrx
- dereg-resp-5xxtx
- dereg-resp-6xxrx
- dereg-resp-6xxtx
- msgsum-subs-resp-3xxrx
- msgsum-subs-resp-3xxtx
- msgsum-subs-resp-4xxrx
- msgsum-subs-resp-4xxtx
- msgsum-subs-resp-5xxrx
- msgsum-subs-resp-5xxtx
- msgsum-subs-resp-6xxrx
- msgsum-subs-resp-6xxtx
- msgsum-resubs-resp-3xxrx
- msgsum-resubs-resp-3xxtx
- msgsum-resubs-resp-4xxrx
- msgsum-resubs-resp-4xxtx
- msgsum-resubs-resp-5xxrx
- msgsum-resubs-resp-5xxtx
- msgsum-resubs-resp-6xxrx
- msgsum-resubs-resp-6xxtx
- msgsum-unsubs-resp-3xxrx
- msgsum-unsubs-resp-3xxtx
- msgsum-unsubs-resp-4xxrx
- msgsum-unsubs-resp-4xxtx
- msgsum-unsubs-resp-5xxrx
- msgsum-unsubs-resp-5xxtx
- msgsum-unsubs-resp-6xxrx
- msgsum-unsubs-resp-6xxtx
- msgsum-notify-attrx
- msgsum-notify-atttx
- msgsum-notify-succrx
- msgsum-notify-succtx
- msgsum-notify-failrx
- msgsum-notify-failtx

- msgsum-notify-resp-3xxrx
- msgsum-notify-resp-3xxtx
- msgsum-notify-resp-400rx
- msgsum-notify-resp-400tx
- msgsum-notify-resp-481rx
- msgsum-notify-resp-481tx
- msgsum-notify-resp-489rx
- msgsum-notify-resp-489tx
- msgsum-notify-resp-4xxrx
- msgsum-notify-resp-4xxtx
- msgsum-notify-resp-500rx
- msgsum-notify-resp-500tx
- msgsum-notify-resp-5xxrx
- msgsum-notify-resp-5xxtx
- msgsum-notify-resp-6xxrx
- msgsum-notify-resp-6xxtx
- msgsum-pub-attrx
- msgsum-pub-atttx
- msgsum-pub-succrx
- msgsum-pub-succtx
- msgsum-pub-failrx
- msgsum-pub-failtx
- msgsum-pub-resp-3xxrx
- msgsum-pub-resp-3xxtx
- msgsum-pub-resp-400rx
- msgsum-pub-resp-400tx
- msgsum-pub-resp-404rx
- msgsum-pub-resp-404tx
- msgsum-pub-resp-412rx
- msgsum-pub-resp-412tx
- msgsum-pub-resp-423rx
- msgsum-pub-resp-423tx
- msgsum-pub-resp-489rx
- msgsum-pub-resp-489tx
- msgsum-pub-resp-4xxrx
- msgsum-pub-resp-4xxtx
- msgsum-pub-resp-500rx
- msgsum-pub-resp-500tx

- msgsum-pub-resp-503rx
- msgsum-pub-resp-503tx
- msgsum-pub-resp-5xxrx
- msgsum-pub-resp-5xxtx
- msgsum-pub-resp-6xxrx
- msgsum-pub-resp-6xxtx
- msgsum-unpub-attrx
- msgsum-unpub-atttx
- msgsum-unpub-succrx
- msgsum-unpub-succtx
- msgsum-unpub-failrx
- msgsum-unpub-failtx
- msgsum-unpub-resp-3xxrx
- msgsum-unpub-resp-3xxtx
- msgsum-unpub-resp-400rx
- msgsum-unpub-resp-400tx
- msgsum-unpub-resp-404rx
- msgsum-unpub-resp-404tx
- msgsum-unpub-resp-412rx
- msgsum-unpub-resp-412tx
- msgsum-unpub-resp-423rx
- msgsum-unpub-resp-423tx
- msgsum-unpub-resp-489rx
- msgsum-unpub-resp-489tx
- msgsum-unpub-resp-4xxrx
- msgsum-unpub-resp-4xxtx
- msgsum-unpub-resp-500rx
- msgsum-unpub-resp-500tx
- msgsum-unpub-resp-503rx
- msgsum-unpub-resp-503tx
- msgsum-unpub-resp-5xxrx
- msgsum-unpub-resp-5xxtx
- msgsum-unpub-resp-6xxrx
- msgsum-unpub-resp-6xxtx
- pres-subs-resp-3xxrx
- pres-subs-resp-3xxtx
- pres-subs-resp-4xxrx
- pres-subs-resp-4xxtx

- pres-subs-resp-5xxrx
- pres-subs-resp-5xxtx
- pres-subs-resp-6xxrx
- pres-subs-resp-6xxtx
- pres-resubs-resp-3xxrx
- pres-resubs-resp-3xxtx
- pres-resubs-resp-4xxrx
- pres-resubs-resp-4xxtx
- pres-resubs-resp-5xxrx
- pres-resubs-resp-5xxtx
- pres-resubs-resp-6xxrx
- pres-resubs-resp-6xxtx
- pres-unsubs-resp-3xxrx
- pres-unsubs-resp-3xxtx
- pres-unsubs-resp-4xxrx
- pres-unsubs-resp-4xxtx
- pres-unsubs-resp-5xxrx
- pres-unsubs-resp-5xxtx
- pres-unsubs-resp-6xxrx
- pres-unsubs-resp-6xxtx
- pres-notify-attrx
- pres-notify-atttx
- pres-notify-succrx
- pres-notify-succtx
- pres-notify-failrx
- pres-notify-failtx
- pres-notify-resp-3xxrx
- pres-notify-resp-3xxtx
- pres-notify-resp-400rx
- pres-notify-resp-400tx
- pres-notify-resp-481rx
- pres-notify-resp-481tx
- pres-notify-resp-489rx
- pres-notify-resp-489tx
- pres-notify-resp-4xxrx
- pres-notify-resp-4xxtx
- pres-notify-resp-500rx
- pres-notify-resp-500tx

- pres-notify-resp-5xxrx
- pres-notify-resp-5xxtx
- pres-notify-resp-6xxrx
- pres-notify-resp-6xxtx
- pres-pub-attrx
- pres-pub-atttx
- pres-pub-succrx
- pres-pub-succtx
- pres-pub-failrx
- pres-pub-failtx
- pres-pub-resp-3xxrx
- pres-pub-resp-3xxtx
- pres-pub-resp-400rx
- pres-pub-resp-400tx
- pres-pub-resp-404rx
- pres-pub-resp-404tx
- pres-pub-resp-412rx
- pres-pub-resp-412tx
- pres-pub-resp-423rx
- pres-pub-resp-423tx
- pres-pub-resp-489rx
- pres-pub-resp-489tx
- pres-pub-resp-4xxrx
- pres-pub-resp-4xxtx
- pres-pub-resp-500rx
- pres-pub-resp-500tx
- pres-pub-resp-503rx
- pres-pub-resp-503tx
- pres-pub-resp-5xxrx
- pres-pub-resp-5xxtx
- pres-pub-resp-6xxrx
- pres-pub-resp-6xxtx
- pres-unpub-attrx
- pres-unpub-atttx
- pres-unpub-succrx
- pres-unpub-succtx
- pres-unpub-failrx
- pres-unpub-failtx

- pres-unpub-resp-3xxrx
- pres-unpub-resp-3xxtx
- pres-unpub-resp-400rx
- pres-unpub-resp-400tx
- pres-unpub-resp-404rx
- pres-unpub-resp-404tx
- pres-unpub-resp-412rx
- pres-unpub-resp-412tx
- pres-unpub-resp-423rx
- pres-unpub-resp-423tx
- pres-unpub-resp-489rx
- pres-unpub-resp-489tx
- pres-unpub-resp-4xxrx
- pres-unpub-resp-4xxtx
- pres-unpub-resp-500rx
- pres-unpub-resp-500tx
- pres-unpub-resp-503rx
- pres-unpub-resp-503tx
- pres-unpub-resp-5xxrx
- pres-unpub-resp-5xxtx
- pres-unpub-resp-6xxrx
- pres-unpub-resp-6xxtx
- reg-subs-resp-3xxrx
- reg-subs-resp-3xxtx
- reg-subs-resp-4xxrx
- reg-subs-resp-4xxtx
- reg-subs-resp-5xxrx
- reg-subs-resp-5xxtx
- reg-subs-resp-6xxrx
- reg-subs-resp-6xxtx
- reg-resubs-resp-3xxrx
- reg-resubs-resp-3xxtx
- reg-resubs-resp-4xxrx
- reg-resubs-resp-4xxtx
- reg-resubs-resp-5xxrx
- reg-resubs-resp-5xxtx
- reg-resubs-resp-6xxrx
- reg-resubs-resp-6xxtx

- reg-unsubs-resp-3xxrx
- reg-unsubs-resp-3xxtx
- reg-unsubs-resp-4xxrx
- reg-unsubs-resp-4xxtx
- reg-unsubs-resp-5xxrx
- reg-unsubs-resp-5xxtx
- reg-unsubs-resp-6xxrx
- reg-unsubs-resp-6xxtx
- reg-notify-attrx
- reg-notify-atttx
- reg-notify-succrx
- reg-notify-succtx
- reg-notify-failrx
- reg-notify-failtx
- reg-notify-resp-3xxrx
- reg-notify-resp-3xxtx
- reg-notify-resp-400rx
- reg-notify-resp-400tx
- reg-notify-resp-481rx
- reg-notify-resp-481tx
- reg-notify-resp-489rx
- reg-notify-resp-489tx
- reg-notify-resp-4xxrx
- reg-notify-resp-4xxtx
- reg-notify-resp-500rx
- reg-notify-resp-500tx
- reg-notify-resp-5xxrx
- reg-notify-resp-5xxtx
- reg-notify-resp-6xxrx
- reg-notify-resp-6xxtx
- reg-pub-attrx
- reg-pub-atttx
- reg-pub-succrx
- reg-pub-succtx
- reg-pub-failrx
- reg-pub-failtx
- reg-pub-resp-3xxrx
- reg-pub-resp-3xxtx

- reg-pub-resp-400rx
- reg-pub-resp-400tx
- reg-pub-resp-404rx
- reg-pub-resp-404tx
- reg-pub-resp-412rx
- reg-pub-resp-412tx
- reg-pub-resp-423rx
- reg-pub-resp-423tx
- reg-pub-resp-489rx
- reg-pub-resp-489tx
- reg-pub-resp-4xxrx
- reg-pub-resp-4xxtx
- reg-pub-resp-500rx
- reg-pub-resp-500tx
- reg-pub-resp-503rx
- reg-pub-resp-503tx
- reg-pub-resp-5xxrx
- reg-pub-resp-5xxtx
- reg-pub-resp-6xxrx
- reg-pub-resp-6xxtx
- reg-unpub-attrx
- reg-unpub-atttx
- reg-unpub-succrx
- reg-unpub-succtx
- reg-unpub-failrx
- reg-unpub-failtx
- reg-unpub-resp-3xxrx
- reg-unpub-resp-3xxtx
- reg-unpub-resp-400rx
- reg-unpub-resp-400tx
- reg-unpub-resp-404rx
- reg-unpub-resp-404tx
- reg-unpub-resp-412rx
- reg-unpub-resp-412tx
- reg-unpub-resp-423rx
- reg-unpub-resp-423tx
- reg-unpub-resp-489rx
- reg-unpub-resp-489tx

- reg-unpub-resp-4xxrx
- reg-unpub-resp-4xxtx
- reg-unpub-resp-500rx
- reg-unpub-resp-500tx
- reg-unpub-resp-503rx
- reg-unpub-resp-503tx
- reg-unpub-resp-5xxrx
- reg-unpub-resp-5xxtx
- reg-unpub-resp-6xxrx
- reg-unpub-resp-6xxtx
- winfo-subs-resp-3xxrx
- winfo-subs-resp-3xxtx
- winfo-subs-resp-4xxrx
- winfo-subs-resp-4xxtx
- winfo-subs-resp-5xxrx
- winfo-subs-resp-5xxtx
- winfo-subs-resp-6xxrx
- winfo-subs-resp-6xxtx
- winfo-resubs-resp-3xxrx
- winfo-resubs-resp-3xxtx
- winfo-resubs-resp-4xxrx
- winfo-resubs-resp-4xxtx
- winfo-resubs-resp-5xxrx
- winfo-resubs-resp-5xxtx
- winfo-resubs-resp-6xxrx
- winfo-resubs-resp-6xxtx
- winfo-unsubs-resp-3xxrx
- winfo-unsubs-resp-3xxtx
- winfo-unsubs-resp-4xxrx
- winfo-unsubs-resp-4xxtx
- winfo-unsubs-resp-5xxrx
- winfo-unsubs-resp-5xxtx
- winfo-unsubs-resp-6xxrx
- winfo-unsubs-resp-6xxtx
- winfo-notify-attrx
- winfo-notify-atttx
- winfo-notify-succrx
- winfo-notify-succtx

- winfo-notify-failrx
- winfo-notify-failtx
- winfo-notify-resp-3xxrx
- winfo-notify-resp-3xxtx
- winfo-notify-resp-400rx
- winfo-notify-resp-400tx
- winfo-notify-resp-481rx
- winfo-notify-resp-481tx
- winfo-notify-resp-489rx
- winfo-notify-resp-489tx
- winfo-notify-resp-4xxrx
- winfo-notify-resp-4xxtx
- winfo-notify-resp-500rx
- winfo-notify-resp-500tx
- winfo-notify-resp-5xxrx
- winfo-notify-resp-5xxtx
- winfo-notify-resp-6xxrx
- winfo-notify-resp-6xxtx
- winfo-pub-attrx
- winfo-pub-atttx
- winfo-pub-succrx
- winfo-pub-succtx
- winfo-pub-failrx
- winfo-pub-failtx
- winfo-pub-resp-3xxrx
- winfo-pub-resp-3xxtx
- winfo-pub-resp-400rx
- winfo-pub-resp-400tx
- winfo-pub-resp-404rx
- winfo-pub-resp-404tx
- winfo-pub-resp-412rx
- winfo-pub-resp-412tx
- winfo-pub-resp-423rx
- winfo-pub-resp-423tx
- winfo-pub-resp-489rx
- winfo-pub-resp-489tx
- winfo-pub-resp-4xxrx
- winfo-pub-resp-4xxtx

- winfo-pub-resp-500rx
- winfo-pub-resp-500tx
- winfo-pub-resp-503rx
- winfo-pub-resp-503tx
- winfo-pub-resp-5xxrx
- winfo-pub-resp-5xxtx
- winfo-pub-resp-6xxrx
- winfo-pub-resp-6xxtx
- winfo-unpub-attrx
- winfo-unpub-atttx
- winfo-unpub-succrx
- winfo-unpub-succtx
- winfo-unpub-failrx
- winfo-unpub-failtx
- winfo-unpub-resp-3xxrx
- winfo-unpub-resp-3xxtx
- winfo-unpub-resp-400rx
- winfo-unpub-resp-400tx
- winfo-unpub-resp-404rx
- winfo-unpub-resp-404tx
- winfo-unpub-resp-412rx
- winfo-unpub-resp-412tx
- winfo-unpub-resp-423rx
- winfo-unpub-resp-423tx
- winfo-unpub-resp-489rx
- winfo-unpub-resp-489tx
- winfo-unpub-resp-4xxrx
- winfo-unpub-resp-4xxtx
- winfo-unpub-resp-500rx
- winfo-unpub-resp-500tx
- winfo-unpub-resp-503rx
- winfo-unpub-resp-503tx
- winfo-unpub-resp-5xxrx
- winfo-unpub-resp-5xxtx
- winfo-unpub-resp-6xxrx
- winfo-unpub-resp-6xxtx
- callrel-from-ue
- callrel-from-nw

- callrel-from-radioloss
- callrel-from-local
- beerrrx
- beerrtx
- tot-sip-msgs-proc
- regreqretx
- invreqretx
- byereqretx
- cancreqretx
- req-retx
- resp-retx
- reqresp-retx
- subsetup<200ms
- subsetup200-400ms
- subsetup400-600ms
- subsetup600-800ms
- subsetup800-1000ms
- subsetup1000-1200ms
- subsetup1200-1400ms
- subsetup1400-1600ms
- subsetup1600-1800ms
- subsetup1800-2000ms
- subsetup2000-2200ms
- subsetup2200-2400ms
- subsetup2400-2600ms
- subsetup2600-2800ms
- subsetup2800-3000ms
- subsetup3-5sec
- subsetup5-7sec
- subsetup7-9sec
- subsetup9-11sec
- subsetup11-13sec
- subsetup13-15sec
- subsetup15-17sec
- subsetup17-19sec
- subsetup19-21sec
- subsetup>21sec
- subdur<1hr

- subdur1-2hr
- subdur2-3hr
- subdur3-4hr
- subdur4-5hr
- subdur5-6hr
- subdur6-7hr
- subdur7-8hr
- subdur8-9hr
- subdur9-10hr
- subdur>10hr
- curr-reg-subs
- active-reg-subs
- curr-sigcomp-subs
- active-sigcomp-subs
- curr-ipsec-subs
- active-ipsec-subs
- active-voip-subs
- curr-presence-subs
- active-presence-subs
- active-im-subs
- dpeca-curr-sessions
- dpeca-tot-sess-init
- dpeca-tot-sess-terminated
- dpeca-tot-sess-failovers
- dpeca-tot-sess-failover-err
- dpeca-tot-msg-received
- dpeca-tot-msg-sent
- dpeca-tot-aar-sent
- dpeca-tot-aaa-received
- dpeca-tot-uncorr-aaa
- dpeca-tot-uncorr-sta
- dpeca-tot-aari-sent
- dpeca-tot-aaai-received
- dpeca-tot-aaai-accepted
- dpeca-tot-aaai-rejected
- dpeca-tot-aaai-timeout
- dpeca-tot-aaru-sent
- dpeca-tot-aaau-received

- dpeca-tot-aaau-timeout
- dpeca-tot-str-sent
- dpeca-tot-sta-received
- dpeca-tot-sta-timeout
- dpeca-tot-asr-received
- dpeca-tot-asa-sent
- dpeca-tot-rar-received
- dpeca-tot-raa-sent
- dpeca-tot-protocol-err
- dpeca-tot-aaa-parse-err
- dpeca-tot-unk-sess-req
- dpeca-tot-unk-cmd-codes
- dpeca-tc-logout
- dpeca-tc-service-not-prov
- dpeca-tc-bad-ans
- dpeca-tc-administrative
- dpeca-tc-link-broken
- dpeca-tc-auth-expired
- dpeca-tc-user-moved
- dpeca-tc-session-timeout
- dpeca-auth-rejected
- dpeca-other-errors
- dpeca-exp-res-invalid-
- service-info
- dpeca-exp-res-filter-
- restrictions
- dpeca-exp-res-req-service-
- not-authorized
- dpeca-exp-res-duplicated-af-session
- dpeca-exp-res-ipcan-session-not-avail

CSCFINTF Schema

The CSCFINT schema was added to track CSCF interfaces.

Added the following stats for this schema:

- sitserrrx
- sitserrtx

Obsoleted Bulk Statistics

GTPP Schema

Following are obsolete now:

- total-gmbsccdr-xmit
- total-gmbsccdr-rexmit
- total-gmbsccdr-accept
- total-gmbscdr-fail

System Schema

Following are obsolete now:

- curr-proxy
- curr-relay-agent
- sess-total-setup
- setup-proxy
- setup-relay-agent
- total-released
- rel-proxy-admin-releases
- rel-proxy-bearer-call-term.
- rel-proxy-lease-exp-policy
- rel-proxy-lease-renew-failure
- rel-proxy-ip-mis-match
- rel-proxy-lease-time-mis-match
- rel-proxy-other-reasons
- rel-relay-admin-releases
- rel-relay-bearer-call-ter.
- rel-relay-lease-time-out
- rel-relay-other-reasons
- discover-tx
- discover-retransmitted
- discover-rx
- discover-retried-rx
- discover-relayed
- discoverd-retried-relayed
- offer-rx
- offer-discarded
- offer-tx
- offer-relayed
- request-tx

- request-retransmitted
- request-rx
- request-renewal-rx
- request-requesting-relayed
- request-renewing-relayed
- ack-rx
- ack-for-inform
- ack-renewing-rx
- ack-tx
- ack-renewing-tx
- ack-relayed
- ack-renewing-relayed
- nak-rx
- nak-for-inform
- nak-tx
- nak-relayed
- decline-tx
- decline-rx
- decline-relayed
- release-tx
- release-rx
- release-relayed
- release-for-relay-call
- inform-tx
- inform-retransmitted
- inform-rx
- inform-relayed
- offer-dis-parse-err
- offer-dis-lease-less-than-min
- offer-dis-lease-greater-than-max
- offer-dis-ip-val-failed
- offer-dis-xid-mismatch
- ack-dis-parse-err
- ack-dis-xid-mis-match
- decline-dis-ip-mis-match
- ip-lease-renewal
- failed-ip-lease-renew
- no-reply-from-server

- server-nak
- ip-addr-mis-match
- lease-mis-match
- cf-cat-adv-pkts-hit
- cf-cat-adv-pkts-block
- cf-cat-auct-pkts-hit
- cf-cat-auct-pkts-block
- cf-cat-clean-pkts-hit
- cf-cat-clean-pkts-block
- cf-cat-cporn-pkts-hit
- cf-cat-cporn-pkts-block
- cf-cat-esrb-pkts-hit
- cf-cat-esrb-pkts-block
- cf-cat-p2p-pkts-hit
- cf-cat-p2p-pkts-block
- cf-cat-phish-pkts-hit
- cf-cat-phish-pkts-block
- cf-cat-radio-pkts-hit
- cf-cat-radio-pkts-block
- cf-cat-sftwre-pkts-hit
- cf-cat-sftwre-pkts-block
- cf-cat-spywre-pkts-hit
- cf-cat-spywre-pkts-block
- cf-cat-susp-pkts-hit
- cf-cat-susp-pkts-block

HAMIPv6 Schema

The following are new for Release 8.1

- admprohreason_badreq
- insufresource_badreq
- bindacksent_senderror
- admprohreason_congcondenied
- ICMPv6_toobigdrop
- bindupddiscard_congdisc
- bindupddiscard_chkerror
- bindupddiscard_iniauthpend
- bindupddiscard_sessnotfound
- bindupddiscard_hamgrnotrea
- bindupddiscard_decfail

- bindupddiscard_invbuflen

Obsoleted Bulk Statistics

The following bulkstats are obsoleted for Release 8.1

HAMIPv6 Schema

- icmpv6_toobiggenerate
- rrqdeny_admprohibit
- rrqdeny_unknownha
- denyreason_simbindexceed
- denyreason_senderror
- denyreason_badreq
- hamipv6-totalsubscriber

Bulk Statistic Enhancements in Release 8.3

This section lists bulk statistic additions and changes in Release 8.3. Detailed information on bulk statistics is located in both the *System Administration Guide* and in the *Statistics and Counters Reference*.

Bulk Statistic Additions

Support for the following bulk statistics has been added:

nat-realm Schema

The new schema nat-realm supports the following variables:

- vpnname
- realmname
- nat-bind-updates
- nat-rlm-bytes-tx
- nat-rlm-flows
- nat-rlm-ip-denied
- nat-rlm-port-denied
- nat-rlm-ttl-ips
- nat-rlm-ips-in-use
- nat-rlm-current-users
- nat-rlm-ttl-port-chunks
- nat-rlm-chunks-in-use

system Schema

The following statistics have been added to the system schema in Release 8.3:

- ikev2-ikesadel
- ikev2-ikesadelreq-sent
- ikev2-ikesadelreq-recv
- ikev2-ikesadelrep-sent
- ikev2-ikesadelrep-recv
- ikev2-curikev2sa
- ikev2-curhalfsa
- ikev2-curconnsa
- ikev2-curestsa
- ikev2-curchildsa
- ikev2-exp-retran
- ikev2-exp-setupnoxchg
- ikev2-exp-setup
- ikev2-exp-lifesoft

- ikev2-exp-lifehard
- ikev2-exp-childsetupnoxchg
- ikev2-exp-childlifesoft
- ikev2-exp-childlifehard
- ikev2-auth-p1succ
- ikev2-auth-p1fail
- ikev2-auth-p1req
- ikev2-auth-p1rsp
- ikev2-auth-p2succ
- ikev2-auth-p2fail
- ikev2-auth-p2req
- ikev2-auth-p2rsp
- ikev2-auth-p2succmd5
- ikev2-auth-p2failmd5
- ikev2-auth-p2succgtc
- ikev2-auth-p2failgtc
- ikev2-auth-failhash
- ikev2-auth-failsign
- ikev2-auth-failmskmiss
- ikev2-auth-failmissanother
- ikev2-xchg-droprspnoikesa
- ikev2-xchg-dropinvrsp
- ikev2-xchg-dropnoninitnoikesa
- ikev2-xchg-dropinvmsgid
- ikev2-xchg-dropinvmajver
- ikev2-xchg-dropikesaerr
- ikev2-xchg-dropunkcrit
- ikev2-xchg-dropretransdisc
- ikev2-notif-cooksent
- ikev2-notif-cookrecv
- ikev2-notif-cookmatch
- ikev2-notif-cooknomatch
- ikev2-notif-multauthsupp
- ikev2-notif-anothauth
- ikev2-rekey-ikesareqsent
- ikev2-rekey-ikesareqrcvd
- ikev2-rekey-ikesarspsent
- ikev2-rekey-ikesarsprcvd

- ikev2-rekey-ikesaignored
- ikev2-rekey-childsareqsent
- ikev2-rekey-childsareqrecv
- ikev2-rekey-childsarspsent
- ikev2-rekey-childsarsprecv
- ikev2-rekey-childsaignored
- ikev2-mobike-sent
- ikev2-mobike-recv
- ikev2-mobike-ignored
- ikev2-misc-ikesacrefail
- ikev2-misc-saflowopfail
- ikev2-notifpaysent-invke
- ikev2-notifpaysent-invmajver
- ikev2-notifpaysent-invmsgid
- ikev2-notifpaysent-invsyn
- ikev2-notifpaysent-noaddsa
- ikev2-notifpaysent-noprop
- ikev2-notifpaysent-tsunaccept
- ikev2-notifpaysent-unsuppcrit
- ikev2-notifpaysent-intfail
- ikev2-notifpayrecv-invke
- ikev2-notifpayrecv-nvmajver
- ikev2-notifpayrecv-invmsgid
- ikev2-notifpayrecv-invsyn
- ikev2-notifpayrecv-noaddsa
- ikev2-notifpayrecv-noprop
- ikev2-notifpayrecv-tsunaccept
- ikev2-notifpayrecv-unsuppcrit
- ikev2-decfail-pktfail
- ikev2-decfail-interr
- ikev2-decfail-iphdr
- ikev2-decfail-udphdr
- ikev2-decfail-ikehdr
- ikev2-decfail-ikehdrpay
- ikev2-decfail-ikehdrinitspi
- ikev2-decfail-ikehdrrspspi
- ikev2-decfail-ikehdrmajver
- ikev2-decfail-ikehdrminver

- ikev2-decfail-ikehdrxchgtyp
- ikev2-decfail-ikehdrrecvflag
- ikev2-decfail-ikehdrlen
- ikev2-decfail-syn
- ikev2-decfail-paysyn
- ikev2-decfail-paylen
- ikev2-decfail-unkcritpay
- ikev2-decfail-toomanypay
- ikev2-decfail-sapaylen
- ikev2-decfail-saprophdr
- ikev2-decfail-saprophdrrecv
- ikev2-decfail-toomanytrans
- ikev2-decfail-saprophdrlen
- ikev2-decfail-toomanyprop
- ikev2-decfail-1stsapropnum
- ikev2-decfail-saprotid
- ikev2-decfail-sapropnum
- ikev2-decfail-translen
- ikev2-decfail-transhdr
- ikev2-decfail-transhdrrecv
- ikev2-decfail-transtype
- ikev2-decfail-transid
- ikev2-decfail-kepaylen
- ikev2-decfail-kedhgrp
- ikev2-decfail-kedhgrplen
- ikev2-decfail-idpaylen
- ikev2-decfail-idpaytype
- ikev2-decfail-authpaylen
- ikev2-decfail-noncepaylen
- ikev2-decfail-notifpaylen
- ikev2-decfail-notifpayspilen
- ikev2-decfail-notifpaynat
- ikev2-decfail-notifpayprotid
- ikev2-decfail-eappaylen
- ikev2-decfail-notifpayrekey
- ikev2-decfail-cppaylen
- ikev2-decfail-notifpaycook
- ikev2-decfail-tspaylen

- ikev2-decfail-cppayattrlen
- ikev2-decfail-tspayrecv
- ikev2-decfail-encrpaylen
- ikev2-decfail-tspaytstype
- ikev2-decfail-unsuppcritpay
- ikev2-decfail-unsuppcertpay
- ikev2-decfail-unsuppnotifprotah
- ikev2-decfail-unsuppauthmeth
- ikev2-decfail-unsupppaycritvid
- ikev2-decfail-unsuppmeth
- ikev2-decfail-unkerr
- ikev2-decfail-unsuppsapayprotah
- ikev2-decfail-unsupptspaytsnum
- ikev2-decfail-unsupptspaytstype
- ikev2-decfail-unsupptspaytsprot
- ikev2-decfail-cppaynoipaddr
- ikev2-decfail-cppayunkattr
- ikev2-decryptfail
- ikev2-decryptfail-hmac
- ikev2-decryptfail-pad
- ikev2-xchg-badmsgid
- ikev2-xchg-badresp
- ikev2-xchg-stalemsgid
- ikev2-xchg-unkerr
- ikev2-xchg-statelookfail
- ikev2-notifrecv-unsuppcritpay
- ikev2-notifrecv-invikespi
- ikev2-notifrecv-invmajver
- ikev2-notifrecv-invsyn
- ikev2-notifrecv-invmsgid
- ikev2-notifrecv-invspi
- ikev2-notifrecv-nopropchosen
- ikev2-notifrecv-invkepay
- ikev2-notifrecv-authfail
- ikev2-notifrecv-singpairreq
- ikev2-notifrecv-noaddsa
- ikev2-notifrecv-intaddrfail
- ikev2-notifrecv-failcpreq

- ikev2-notifrecv-tsunaccept
- ikev2-notifrecv-invsel
- ikev2-notifrecv-unacceptaddr
- ikev2-notifrecv-multiauthsupp
- ikev2-notifrecv-anothauthfoll
- ikev2-notifrecv-unexpectnat
- ikev2-notifrecv-macauthfail
- ikev2-notifrecv-hsserrusrunk
- ikev2-notifrecv-initcont
- ikev2-notifrecv-windsiz
- ikev2-notifrecv-addtsposs
- ikev2-notifrecv-ipcompsupp
- ikev2-notifrecv-natdetsrcip
- ikev2-notifrecv-natdetdstip
- ikev2-notifrecv-cookie
- ikev2-notifrecv-usetransmode
- ikev2-notifrecv-httpcertsupp
- ikev2-notifrecv-rekeysa
- ikev2-notifrecv-nonfirstfragalso
- ikev2-notifrecv-mobikesupp
- ikev2-notifrecv-addip4addr
- ikev2-notifrecv-addip6addr
- ikev2-notifrecv-noaddaddr
- ikev2-notifrecv-updsaaddr
- ikev2-notifrecv-cookie2
- ikev2-notifrecv-nonatallow
- ikev2-notifrecv-other
- ikev2-notifrecv-sipfallbnotallow
- ikev2-notifrecv-esptfcpadnotsupp
- ikev2-notifrecv-congrejrecv
- ikev2-cert-reqsent
- ikev2-cert-reqrecv
- ikev2-cert-sent
- ikev2-cert-recv
- ike-udpflows
- ike-cookieflows
- ike-txpackets
- ike-rxpackets

- ike-reqrecv
- ike-udpflowpackets
- ike-cookieflowpackets
- crypto-txesppacket
- crypto-txespoctet
- crypto-txahpacket
- crypto-txahoctet
- crypto-rxesppacket
- crypto-rxespoctet
- crypto-rxahpacket
- crypto-rxahoctet
- crypto-errauthpacket
- crypto-errauthoctet
- crypto-errbadrecpacket
- crypto-errbadrecoctet
- crypto-errdiscpacket
- crypto-errdiscoctet
- crypto-errignpacket
- crypto-errignoctet
- crypto-errunderrunpacket
- crypto-errunderrunoctet
- crypto-errinvpacket
- crypto-errinvoctet
- crypto-errreplaypacket
- crypto-errreplayoctet

PDIF schema

The following statistics have been added to the PDIF schema in Release 8.3:

- sess-distysetuptimeout
- ipsec-violpacket

CDR Enhancements

This section lists new GTPP dictionaries and changes in Release 8.1. Refer to the *AAA Interface Configuration and Reference* for details.

- custom14: Custom dictionary, now with support for S-CDR
- custom21: Custom dictionary, with support for G-CDR
- custom22: Custom dictionary, with support for G-CDR
- custom23: Custom dictionary, with support for S-CDR

Command Enhancements

None for this release.

New Commands

None for this release.

Diameter AVPs in Release 8.0

This section lists additions and changes to Diameter AVPs in Release 8.0. Refer to the *AAA Interface Configuration and Reference* for details on the attribute value pairs supported by the system.

New Attributes

- BCID
- Acct-Realtime-Required
- Additional-MBMS-Trace-Info
- Alternative-APN
- BM-Address
- BM-Cause-Code
- BM-Correlation-ID
- BM-Information
- BM-Type
- Carrier-ID
- Correlate-Reason
- Dialog-Id
- Digest-Algorithm
- Digest-Auth-Param
- Digest-Domain
- Digest-HA1
- Digest-QoP
- Digest-Realm
- Direction
- Direct-Message
- Element-ID
- Element-Type
- Event-Message-Type
- Experimental-Result-Code
- Expires
- FDR-Reason
- First-Packet-Direction
- GMT-Timezone-Offset
- Group-ID
- HBM-Address
- HOA-Session-ID
- IMS-Communication-Service-Identifier

- Initial-CellSector-ID
- IN-Service
- IPGW-Address
- Last-CellSector-ID
- Last-CellSector-Location
- LI-Information
- MBMS-2G-3G-Indicator
- MBMS-BMSC-SSM-IP-Address
- MBMS-BMSC-SSM-IPv6-Address
- MBMS-Counting-Information
- MBMS-Required-QoS
- MBMS-Service-Area
- MBMS-Service-Type
- MBMS-Session-Duration
- MBMS-Session-Identity
- MBMS-Session-Repetition-number
- MBMS-StartStop-Indication
- MBMS-Time-To-Data-Transfer
- MBMS-User-Data-Mode-Indication
- New-Dialog-Id
- Nortel-Data-Reference
- RAI
- Required-MBMS-Bearer-Capabilities
- SIP-Digest-Authenticate
- SIP-Message
- SN-Bandwidth-Control
- Start-Time
- Stop-Time
- Tap-Id
- TMGI
- Transport-Protocol
- VBM-Address
- VOA-Session-ID

Modified Attributes

- 3GPP-RAT-Type-Enum
- Event-Trigger
- IP-CAN-Type
- Max-Requested-Bandwidth-DL
- Max-Requested-Bandwidth-UL
- QoS-Class-Identifier

Removed Attributes

No attributes were removed from Release 8.0.

Diameter AVPs in Release 8.1

IMPORTANT

This section lists additions and changes to Diameter AVPs in Release 8.1.

Refer to the *AAA Interface Administration and Reference* for details on the attribute value pairs supported by the system.

New Attributes

- Acceptable-Service-Info
- Binding-Information
- Binding-Input-List
- Binding-Output-List
- BSID
- Customer-Id
- DIR
- Home-Agent
- IP-Version-Authorized
- Latching-Indication
- MBMS-BMSC-SSM-IP-Address
- MBMS-BMSC-SSM-IPv6-Address
- MBMS-GGSN-Address
- MBMS-GGSN-IPv6-Address
- MBMS-User-Data-Mode-Indication
- Multiple-Auth-Profile
- Multiple-Auth-Support
- Paging-Group-Id
- Port-Number
- Reservation-Class
- Revalidation-Time
- Rule-Activation-Time
- Rule-Deactivation-Time
- Rule-Failure-Code
- Rule-Reason-Code
- SDP-Answer-Timestamp
- SDP-Offer-Timestamp
- SDP-TimeStamps
- Service-Class

- Service-Info-Status
- Session-Release-Cause
- SN-Bandwidth-Control
- SN-Firewall-Policy
- SN-Monitoring-Key
- SN-Service-Flow-Detection
- SN-Traffic-Policy
- SN-Transparent-Data
- SN-Usage-Monitoring
- SN-Usage-Monitoring-Control
- SN-Usage-Volume
- Transport-Class
- UAR-Flags
- V4-Transport-Address
- V6-Transport-Address

Modified Attributes

- 3GPP-RAT-Type-Enum
- Bearer-Control-Mode
- Charging-Rule-Install
- Charging-Rule-Report
- Early-Media-Description
- Event-Trigger
- Experimental-Result-Code
- Flow-Status
- IP-Version-Authorized
- Max-Requested-Bandwidth-DL
- Max-Requested-Bandwidth-UL
- TFT-Packet-Filter-Information

Removed Attributes

No attributes were removed from Release 8.1.

RADIUS Attributes in Release 8.0

This section lists additions and changes to RADIUS attributes in Release 8.0. Refer to the *AAA Interface Reference* for details on the attributes supported by the system.

New Attributes

- Access-Request-Response-Average-Round-Trip-Time
- Accounting-Response-Average-Round-Trip-Time
- 3GPP2-MIP6-Authenticator
- 3GPP2-MIP6-CoA
- 3GPP2-MIP6-HA
- 3GPP2-MIP6-HoA
- 3GPP2-MIP6-HoA-Not-Authorized
- 3GPP2-MIP6-Home-Address
- 3GPP2-MIP6-Home-Agent
- 3GPP2-MIP6-Home-Link-Prefix
- 3GPP2-MIP6-MAC-Mobility-Data
- 3GPP2-MIP6-Mesg-ID
- 3GPP2-MIP6-Session-Key
- DNS
- FA-RK-SPI
- PMIP-Authenticated-Nwk-Id
- SN1-DNS-Proxy-Use-Subscr-Addr
- SN1-Ecs-Data-Volume
- SN1-Firewall-Enabled
- SN1-MIP-Reg-Lifetime-Realm
- SN1-QoS-Traffic-Policy
- SN1-Tunnel-Gn
- SN-DNS-Proxy-Use-Subscr-Addr
- SN-Ecs-Data-Volume
- SN-Firewall-Enabled
- SN-MIP-Reg-Lifetime-Realm
- SN-QoS-Traffic-Policy
- SN-Sec-IP-Pool-Name
- SN-Tunnel-Gn

Modified Attributes

- SN1-Disconnect-Reason
- SN1-PPP-Progress-Code
- SN1-QoS-Traffic-Policy
- SN1-Tp-Uplk-Violate-Action
- SN-Disconnect-Reason
- SN-PPP-Progress-Code
- SN-QoS-Tp-Dnlk
- SN-QoS-Tp-Uplk
- SN-QoS-Traffic-Policy
- SN-Tp-Uplk-Violate-Action

Removed Attributes

- SN-Firewall-Policy
- SN1-Firewall-Policy

RADIUS Attributes in Release 8.1

IMPORTANT

This section lists additions and changes to RADIUS attributes in Release 8.1.

Refer to the *AAA Interface Administration and Reference* for details.

New Attributes

- SN1-NAT-IP-Address
- SN1-Transparent-Data
- SN-Acs-Credit-Control-Group
- SN-Bandwidth-Policy
- SN-CBB-Policy
- SN-Firewall-Policy
- SN-NAT-IP-Address
- SN-Sec-IP-Pool-Name
- SN-Transparent-Data
- UAR-Flags
- WiMAX-Packet-Flow-Descriptor-V2
- WiMAX-PPAC
- WiMAX-PPAQ
- WiMAX-Session-Term-Capability

Modified Attributes

- 3GPP2-Remote-IPv4-Addr-Octets
- Session-Timeout
- SN1-Disconnect-Reason
- SN1-PPP-Progress-Code
- SN1-Prepaid
- SN1-QoS-Traffic-Policy
- SN1-Tp-Dnlk-Exceed-Action
- SN1-Tp-Dnlk-Violate-Action
- SN1-Tp-Uplk-Exceed-Action
- SN1-Tp-Uplk-Violate-Action
- SN-CSCF-Rf-SDP-Media-Components
- SN-Disconnect-Reason
- SN-PPP-Progress-Code

- SN-Prepaid
- SN-QoS-Traffic-Policy
- SN-Tp-Dnlk-Exceed-Action
- SN-Tp-Dnlk-Violate-Action
- SN-Tp-Uplk-Exceed-Action
- SN-Tp-Uplk-Violate-Action
- WiMAX-PPAQ
- WiMAX-Prepaid-Indicator
- WiMAX-QoS-Descriptor

Removed Attributes

No attributes were removed from Release 8.1.

RADIUS Attributes in Release 8.3

IMPORTANT

This section lists additions and changes to RADIUS attributes in Release 8.3.

Refer to the *AAA Interface Administration and Reference* for details.

New Attributes

No new attributes for this release.

Modified Attributes

- SN1-MIP-Send-Term-Verification
- SN-MIP-Send-Term-Verification

Removed Attributes

No attributes were removed from Release 8.3.

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. These additions and modifications are for Release 8.0 unless specifically noted for 8.1.

New Commands

Common Commands - New in Release 8.0

The following common commands are new in Release 8.0.

show diameter message-queue

This command displays Diameter message queue statistics.

CLI (Exec Mode)

show diameter message-queue counters { inbound | outbound } [endpoint *endpoint_name* **[peer-host** *peer_id* **[peer-realm** *realm_id* **]] | session-id** *session_id* **] [| { grep** *grep_options* **| more }]**

Web Element Manager Path

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

show multicast-sessions all

New description table with counter description for output of this command added.

CLI (Exec Mode)

show show multicast-sessions [*command_keyword* **] [** *filter_keywords* **] [| { grep** *grep_options* **| more }**

Web Element Manager Path

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

dns-client

New command added to test and perform DNS query on the basis of specified DNS client name, DNS query domain name, and type of query.

CLI (Exec Mode)

dns-client *dns_client_name* **[query-type { A | AAAA | NAPTR | SRV }] query-name** *query_domain_name*

Web Element Manager Path

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

Common Commands - New in Release 8.1

show hd raid

A new show command has been created to show the RAID created on the ST40 SMC hard disks.

CLI (Exec Mode)

show hd raid [verbose]

Web Element Manager Path

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

show ipv6 interface summary

Presents a summary of all configured ipv6 interfaces

CLI (Exec Mode)

show ipv6 interface summary

Web Element Manager Path

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

show ipv6 neighbor

A new command to show connected IPv6 neighbor addresses

CLI (Exec Mode)

show ipv6 neighbors [ipv6 address]

Web Element Manager Path

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

show ipv6 route

Shows ipv6 route to next gateway

CLI (Exec Mode)

show ipv6 route [*ipv6 prefix/prefix length* **]**

Web Element Manager Path

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

show port info

This command has been modified to include search capabilities for VLAN ID

The output for this command has been modified to show LACP.

CLI (Exec Mode)

show port info *slotnum/portnum*

Web Element Manager Path

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

show port table

The output of this table is modified when ports are included in a Link Aggregation Group. The Redundant With column will show “LAG” for each aggregated port. If an aggregated port is collecting and distributing data, a “+” sign appears next to the LAG entry. If the port is collecting but not distributing data, a “-” appears instead.

CLI (Exec Mode)

show port table

Web Element Manager Path

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

show subscribers

The output of this command is modified to display following counters with various filter keywords:

```
in packet dropped due to zero mbr
out packet dropped due to zero mbr
```

CLI (Exec Mode)

show subscribers

show subscribers full

show subscribers full username

show subscribers counters username

show subscribers ggsn-only full

show subscribers summary

show subscribers ggsn-only summary

Web Element Manager Path

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

show configuration errors

New keyword IPMS is added with this command to display the errors in configuration for IPMS service on an AGW.

CLI (Exec Mode)

show configuration errors [section { aaa-config | active-charging | asngw-service | asnpc-service | closed-rp-service | cscf-service | diameter | fa-service | ggsn-service | ha-service | imssh-service | ipms | ipsg-service | lac-service | lns-service | pdif-service | pdsn-service | policy-grp-config | subscriber-config }] [verbose] [| { grep *grep_options* **| more }]**

Web Element Manager Path

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

show ipms status

New command added to display the IPMS support related statistics of IPMS client service on AGW and IPMs servers configured for this support on an AGW.

CLI (Exec Mode)

show ipms status [summary | all | server address *ip_address*]

Web Element Manager Path

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

Common Commands - New in Release 8.3

clear radius accounting archive

This command clears archived RADIUS accounting messages associated with a AAA group, or all the archived RADIUS accounting messages in the context in which the command is executed depending on the option chosen. The scope of the command is limited to the context in which it is executed including for local context.

CLI (Exec Mode)

clear radius accounting archive { all | radius group *group_name* **} [-noconfirm]**

Web Element Manager Path

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

CF Commands - New in Release 8.0

All of the following CF commands are new in Release 8.0.

clear content-filtering category statistics

This new command added to the Exec mode. This command clears all content filtering category statistics for database, SRDB manager instance, and database volume.

CLI (Exec Mode)

`clear content-filtering category statistics [ all | facility srdbmgr [ all | instance` *`instance_value`* **`] |`** **volume number** *`volume_num`***]**

Web Element Manager Path

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

CF Commands - New in Release 8.1

IMPORTANT

All of the following CF commands are only available in Release 8.1.

clear active-charging url-blacklisting statistics

This command clears URL Blacklisting feature related statistics.

CLI (Exec Mode)

clear active-charging url-blacklisting statistics [rulebase 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 content-filtering category policy-id

This command displays Content Filtering category policy definitions. This command replaces the **show content-filtering category policy-id** command available on StarOS 8.0 and earlier.

CLI (Exec Mode)

show active-charging content-filtering category policy-id { all | id *policy_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 url-blacklisting statistics

This command displays URL Blacklisting statistics.

CLI (Exec Mode)

show active-charging url-blacklisting statistics [rulebase { all | name *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 url-blacklisting database

This command displays URL Blacklisting static database configurations.

CLI (Exec Mode)

show url-blacklisting database [all | url *url* **| facility acsmgr { all | instance** *instance* **}] [| { grep** *grep_options* **| more }]**

Web Element Manager Path

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

show url-blacklisting url

This command displays URL information of the URLs present in the Blacklisting database.

CLI (Exec Mode)

show url-blacklisting url *url* **[generic | exact-match] [| { grep** *grep_options* **| more }]**

Web Element Manager Path

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

ECS Commands - New in Release 8.0

clear active-charging group-of-ruledefs statistics

This command clears statistical information related to Active Charging Service group of ruledefs.

CLI (Exec Mode)

clear active-charging group-of-ruledefs statistics [name *group_of_ruledefs* **] [| { grep** *grep_options* **| more }]**

Web Element Manager Path

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

show active-charging group-of-ruledefs

This command displays information on group of ruledefs configured in a service.

CLI (Exec Mode)

show active-charging group-of-ruledefs { all | name *group_of_ruledefs* **} [service name** *service* **] | statistics name** *group_of_ruledefs* **} [| { grep** *grep_options* **| more }]**

Web Element Manager Path

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

show active-charging packet-filter

This command displays information on packet filters configured in a service.

CLI (Exec Mode)

show active-charging packet-filter { all | name *packet_filter* **} [service name** *service_name* **] [| { grep** *grep_options* **| more }]**

Web Element Manager Path

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

ECS Commands - New in Release 8.1

The following ECS commands are new in Release 8.1.

show active-charging timedef

This command displays the details of timeslots configured in specified time definition(s).

CLI (Exec Mode)

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

Web Element Manager Path

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

Firewall Commands - New in Release 8.0

The following new Firewall commands are available in Release 8.0:

clear active-charging firewall statistics

This command clears Stateful Firewall statistics.

CLI (Exec Mode)

clear active-charging firewall statistics [callid *call_id* **| domain-name** *domain_name* **| protocol { icmp | ip | other | tcp | udp } | username** *user_name* **] [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.

show active-charging firewall statistics

This command displays Stateful Firewall statistics.

CLI (Exec Mode)

show active-charging firewall statistics [callid *call_id* **| domain-name** *domain_name* **| 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.

threshold fw-deny-rule

This command configures thresholds for Stateful Firewall Deny Rule.

CLI (Global Configuration Mode)

threshold fw-deny-rule *high_thresh* **[clear** *low_thresh* **]**

default threshold fw-deny-rule

Web Element Manager Path

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

threshold fw-dos-attack

This command configures thresholds for Stateful Firewall DoS attacks.

CLI (Global Configuration Mode)

threshold fw-dos-attack *high_thresh* **[clear** *low_thresh* **]**

default threshold fw-dos-attack

Web Element Manager Path

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

threshold fw-drop-packet

This command configures thresholds for Stateful Firewall drop packets.

CLI (Global Configuration Mode)

threshold fw-drop-packet *high_thresh* **[clear** *low_thresh* **]**

default threshold fw-drop-packet

Web Element Manager Path

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

threshold fw-no-rule

This command configures thresholds for Stateful Firewall no rules.

CLI (Global Configuration Mode)

threshold fw-no-rule *high_thresh* **[clear** *low_thresh* **]**

default threshold fw-no-rule

Web Element Manager Path

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

Firewall Commands - New in Release 8.1

The following new Firewall commands are available in Release 8.1:

clear active-charging firewall track-list

This command clears the list of servers being tracked for involvement in any Denial-of-Service (DOS) attacks.

CLI (Exec Mode)

`clear active-charging firewall track-list attacking-servers`

Web Element Manager Path

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

show active-charging firewall track-list

This command displays the list of servers being tracked for involvement in any Denial-of-Service (DOS) attacks.

CLI (Exec Mode)

`show active-charging firewall track-list attacking-servers [ | { grep` *`grep_options`* **`| more } ]`**

Web Element Manager Path

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

GGSN Commands - New in Release 8.0

show gtpp group

This new command added to the Exec mode. This command show all GTPP server group configuration information for a specific server group or all server groups configured in a context including default group.

CLI (Exec Mode)

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

Web Element Manager Path

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

GGSN Commands - New in Release 8.1

show mbms bearer-service

New command added to display counters for MBMS related bearer service statistics:

CLI (Exec Mode)

show mbms bearer-service [all | apn apn_name mcast-addr *ip_address* **| service-type { broadcast | multicast } | full | instance** *instance_id* **| summary] + [| { 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

New keyword **streaming** added to this command to show statistics/counters when CDRs stored on HDD for streaming mode.

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.

HA Commands - New in Release 8.0

Currently, there are no new HA commands in Release 8.0.

HA Commands - New in Release 8.1

Currently, there are no new HA commands in Release 8.1.

NAT Commands - New in Release 8.3

The following new NAT commands are available in Release 8.3:

clear active-charging nat statistics

This command clears NAT realm statistics.

CLI (Exec Mode)

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

Web Element Manager Path

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

nat-realm schema

This command creates and configures Network Address Translation (NAT) realm statistics schema.

CLI (Bulk Statistics Configuration Mode)

nat-realm schema *schema_name* **format** *format_string*

no nat-realm schema *schema_name*

Web Element Manager Path

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

show active-charging nat statistics

This command displays NAT realm statistics.

CLI (Exec Mode)

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

Web Element Manager Path

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

show bulkstats variables nat-realm

This command displays available Network Address Translation (NAT) bulk statistics variables.

CLI (Exec Mode)

show bulkstats [[data] | [schemas] | [variables [apn | asngw | asnpc | bcmcs | card | closedrp | common | context | cscf | ecs | fa | gtpc | gtpp | ha | ippool | ipsg | lac | nat-realm | pdif | port | ppp | radius | rp | sccp | sgsn | sgtp | ss7link | ss7rd | system | vpn] [obsolete]] [| { grep *grep_options* **| more }]]**

Web Element Manager Path

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

threshold nat-port-chunks-usage

This command configures the NAT port chunk utilization threshold settings.

CLI (Global Configuration Mode)

threshold nat-port-chunks-usage *high_thresh* **[clear** *low_thresh* **]**

default threshold nat-port-chunks-usage

Web Element Manager Path

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

threshold poll nat-port-chunks-usage

This command configures the polling interval over which to measure the NAT port chunks usage thresholding value.

CLI (Global Configuration Mode)

threshold poll nat-port-chunks-usage interval *30*

Web Element Manager Path

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

snmp trap { enable | suppress } ThreshClearNATPortChunksUsage

This command enables/suppresses generation of the ThreshClearNATPortChunksUsage trap.

CLI (Global Configuration Mode)

snmp trap enable ThreshClearNATPortChunksUsage

snmp trap suppress ThreshClearNATPortChunksUsage

Web Element Manager Path

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

snmp trap { enable | suppress } ThreshNATPortChunksUsage

This command enables/suppresses generation of the ThreshNATPortChunksUsage trap.

CLI (Global Configuration Mode)

snmp trap enable ThreshNATPortChunksUsage

snmp trap suppress ThreshNATPortChunksUsage

Web Element Manager Path

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

PDIF Commands - New in Release 8.0

PDIF is not supported in Release 8.0.

PDIF Commands - New in Release 8.1

The following new PDIF commands are available in Release 8.1.

show certificate

A new command to show the content of a configured X.509 trusted certificate

CLI (Exec Mode)

`show certificate`

Web Element Manager Path

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

show crypto ikev2-ikesa security-associations summary table

show crypto ikev2-ikesa security-associations summary table added to Exec Mode. Includes SA lifetime/lifetime remaining stats.

CLI (Exec Mode)

`show crypto ikev2-ikesa security-associations summary`

Web Element Manager Path

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

show crypto managers instance

This show command has been modified to show trusted certificate information. There is also a new variable do define the instance in question: *`instance_num`*

CLI (Exec Mode)

`show crypto managers instance` *`instance_num`*

Web Element Manager Path

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

show crypto managers summary

The **`show crypto managers summary`** command now show stats per service ip address for each manager.

CLI (Exec Mode)

`show crypto managers summary`

Web Element Manager Path

Performance | IPSecurity | crypto managers summary

show crypto statistics ikev2

A new command to show crypto statistics for IKEv2 for a particular pdif service

Show crypto statistics has been changed to add the keywords s**`ervice-ip-address`** and **`service-name`**. ikev1 has been removed as an option.

CLI (Exec Mode)

show crypto statistics ikev2 [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.

PDSN Commands - New in Release 8.0

show credit-control session

This command shows the credit-control session information based on keywords.

CLI (Exec Mode)

show credit-control session [all | callid | full | mdn | nai | summary] [| { grep *grep_options* **| more }]**

Web Element Manager Path

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

show credit-control statistics

This command shows the credit-control statistics.

CLI (Exec Mode)

show credit-control statistics cc-service <*name*>

Web Element Manager Path

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

PDSN Commands - New in Release 8.1

Currently, there are no new PDSN commands in Release 8.1.

SGSN Commands - New in Release 8.0

show network-service-entity

Displays information regarding the network service entities (NSEs) in the network.

CLI (Exec Mode)

show network-service-entity { consolidated-status | fr-config | ip-config }

Web Element Manager Path

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

show sgsn-operator-policy full

Displays the configuration information for one or all SGSN operator policies.

CLI (Exec Mode)

show sgsn-operator-policy full { all | name }

Web Element Manager Path

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

SGSN Commands - New in Release 8.1

clear super-charger

Deletes the subscription data for one or all subscribers with valid super charger configurations.

CLI (Exec Mode)

```
clear super-charger { imsi <imsi> | all }
```

Web Element Manager Path

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

show freeze-ptmsi

Command indicates whether an IMSI is associated with a frozen P-TMSI in the freeze-ptmsi list.

CLI (Exec Mode)

```
show freeze-ptmsi imsi <imsi>
```

Web Element Manager Path

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

show super-charger

Lists subscribers with valid super charger configuration.

CLI (Exec Mode)

```
show super-charger { imsi <imsi> | all }
```

Web Element Manager Path

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

Modified Commands

Common Commands - Modified in Release 8.0

The following common commands have been modified in Release 8.0.

clear cscf-service

The **li-packet-cable statistics** option was added to the **clear cscf-service** command. This option clears Lawful Intercept statistics.

CLI (Exec Mode)

clear cscf-service [li-packet-cable statistics | statistics [name *service_name* **| vpn-name** *name* **]]**

Web Element Manager Path

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

clear subscribers

The **firewall { not-required | required }** option has been added to this command. This option clears information for the specified subscribers. The **firewall-policy** *fw_policy_name* keyword is obsoleted.

CLI (Exec Mode)

clear subscribers firewall { not-required | required }

Web Element Manager Path

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

clear subscribers gtp-version

The gtp-version option has been added to this command. This option clears information for the specified subscribers.

CLI (Exec Mode)

clear subscribers gtp-version

Web Element Manager Path

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

monitor subscriber type

The monitor subscriber functions have been enhanced to support the monitoring of the following new types:

- 1xrtt
- asngw
- closedrp
- evdorev0
- evdoreva

- ggsn
- ha
- ipsg
- lns
- pdif

CLI (Exec Mode)

monitor subscriber type [1xrtt | asngw | asnpc | closedrp | evdorev0 | evdoreva | ggsn | ha | ipsg | lns | pdif } next-call

Web Element Manager Path

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

show aaa

The **group { all | name** *aaa_group* **}** option was added to this command. This option displays AAA group configurations for a specified AAA group, or for all AAA groups.

CLI (Exec Mode)

show aaa { group { all | name *aaa_group* **} | local counters } [| { grep** *grep_options* **| more }]**

Web Element Manager Path

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

show cscf-service

The **li-packet-cable statistics** option was added to the **show cscf-service** command. This option displays Lawful Intercept statistics.

CLI (Exec Mode)

show cscf-service { all [counters] | diameter policy_control statistics | grey-list name *name* **| li-packet-cable statistics | name** *service_name* **[counters] | statistics name** *service_name* **[vpn-name** *name* **] | subscription name** *service_name* **} [| { grep** *grep_options* **| more }]**

Web Element Manager Path

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

show radius counters all

This command displays RADIUS accounting and/or authentication statistics information. The output of this command includes the following new fields:

- Access-Request Response Average Round Trip Time
- Accounting-Response Average Round Trip Time

Also, in this command's output, the "Authentication server address" and "Accounting server address" fields now include the following information:

- IP address
- Port number

- Server group name

CLI (Exec Mode)

show radius counters { all | radius group *group_name* **all | server** *ip_address* **[port** *number* **] | summary [all-contexts [verbose]] } [| { grep** *grep_options* **| more }]**

Web Element Manager Path

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

show session subsystem facility aaamgr all

The output of this command includes the following new fields:

- Total radius authorization responses dropped
- Total radius accounting responses dropped

CLI (Exec Mode)

show session subsystem facility aaamgr all

Web Element Manager Path

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

show subscribers

The **firewall { not-required | required }** option was added to this command. This option displays information for the specified subscribers. The **firewall-policy** *fw_policy_name* keyword is obsoleted.

CLI (Exec Mode)

show subscribers firewall { not-required | required }

Web Element Manager Path

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

show subscribers

The following new keywords has been added to this command. This option displays information for the specified subscribers in SGSN service:

- sgsn-only [partial [qos [requested | negotiated]+]
- rnc id *rnc_id*
- ggsn *ip_address*

CLI (Exec Mode)

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

Web Element Manager Path

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

show subscribers full

The output of this command includes the following new fields:

- local ip addr
- ROHC cid-mode (local/remote)
- ROHC max-cid (local/remote)
- ROHC mrru (local/remote)
- ROHC max-hdr (local/remote)

CLI (Exec Mode)

show subscribers full

Web Element Manager Path

Click Performance | Subscriber Information | Subscriber Information tab.

show subscribers gtp-version

The **gtp-version** option has been added to this command. This option displays information for the specified subscribers.

CLI (Exec Mode)

show subscribers gtp-version

Web Element Manager Path

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

threshold monitoring

The **firewall** keyword has been added to this command. This command enables thresholding for the specified option.

CLI (Global Configuration Mode)

[no | default] threshold monitoring { aaa-acct-archive-size | aaa-acct-failure | aaa-auth-failure | aaa-retry-rate | aaamgr-request-queue | asngw | call-setup | cpu-resource | cpu-session-throughput | content-filtering | cscf-service | ecs | fa-service | firewall | ha-service | ipsec | license | packets-filtered-dropped | packets-forwarded-to-cpu | pdsn-service | pdif | subscriber | system}

Web Element Manager Path

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

threshold poll

This command configures the polling interval over which to count or measure the thresholding value. The following keywords have been added to this command:

- fw-deny-rule
- fw-dos-attack
- fw-drop-packet
- fw-no-rule

CLI (Global Configuration Mode)

[default] threshold poll { 10sec-cpu-utilization | a11-rrp-failure | a11-rrq-msg-discard | a11-rac-msg-discard | aaa-acct-archive-size | aaa-acct-failure | aaa-acct-failure-rate | aaa-auth-failure | aaa-auth-failure-rate | aaa-retry-rate | aaamgr-request-queue | active-subscriber | all-ppp-send-discard | available-ip-pool-group | call-reject-no-resource | call-setup | call-setup-failure | cpu-available-memory | cpu-load | cpu-orbs-crit | cpu-orbs-warn | cpu-session-throughput | cpu-utilization | cscf-service-route-failures | dereg-reply-error | fa-reg-reply-error | fw-deny-rule | fw-dos-attack | fw-drop-packet | fw-no-rule | ha-init-rrq-rcvd-rate | ha-svc-init-rrq-rcvd-rate| ip-pool-free | ip-pool-hold | ip-pool-release | ip-pool-used | ipsec-call-req-rej | ipsec-ike-failrate | ipsec-ike-failures | ipsec-ike-requests | ipsec-tunnels-established | ipsec-tunnels-setup | license-remaining-session | mgmt-cpu-memory-usage interval | mgmt-cpu-utilization | packets-filtered-dropped | packets-forwarded-to-cpu | pdif-current-sessions | pdif-current-active-sessions | pdsn-init-rrq-rcvd-rate | per-service-ggsn-sessions | per-service-ha-sessions | per-service-lns-sessions | per-service-pdsn-sessions | per-service-sgsn-sessions | per-service-sgsn-pdp-sessions | port-high-activity | port-rx-utilization | port-tx-utilization | ppp-setup-fail-rate | reg-reply-error | rereg-reply-error | rp-setup-fail-rate | storage-utilization | total-ggsn-sessions | total-ha-sessions | total-lns-sessions | total-pdsn-sessions | total-sgsn-sessions | total-sgsn-pdp sessions | total-subscriber } interval *time*

Web Element Manager Path

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

show port table

The introduction of the Quad Gig-E line Card on the ST40 means that additional information is available in the Redundant With... column whenever the port is used in a link aggregation. The following is added to the Show Port Table output in the *Show Command Outputs* chapter in the *Counters and Statistics Reference*:

Extra information is shown in the “Redundant With” column when the port is in a Link Aggregation using the four-port Quad Gig-E line card (QGLC) in an ST40. It now shows LAG and the redundant card/port detail and a + character if the port is selected and a - character if it is not selected.

Web Element Manager Path

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

Common Commands - Modified in Release 8.1

IMPORTANT

The following common commands have been modified in Release 8.1.

clear subscribers

This command clears information for specified subscriber sessions. The **nat** keyword was added to this command. This enables to clear information for subscribers with NAT required or not required, as specified.

CLI (Exec Mode)

clear subscribers [*keywords* **] [verbose] [-noconfirm] [| { grep** *grep_options* **| more }]**

Web Element Manager Path

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

show dhcp-service name

The output of this command now includes the “DHCP Client Identifier” field, which indicates the behavior relating to inclusion of client identifier DHCP option in DHCP messages.

CLI (Exec Mode)

show dhcp-service { all | name *svc_name* **}**

Web Element Manager Path

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

show diameter aaa-statistics

This command displays Diameter AAA statistics. The output of this command includes the following new fields:

- Session Stats
  - Total Sessions
  - Freed Sessions
  - Session Timeouts
  - Active Sessions

CLI (Exec Mode)

show diameter aaa-statistics [all | [group *group_name* **] server** *server_name* **] [| { grep** *grep_options* **| more }]**

Web Element Manager Path

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

show diameter authentication servers

This command displays Diameter Authentication server information. The output of this command has been modified, and now displays the number of instances between the Diameter server and AAA Manager in up and down states.

CLI (Exec Mode)

show diameter authentication servers [aaa-group *group_name* **]**

Web Element Manager Path

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

show diameter peers full all

The output of this command includes the following new fields. These fields are displayed only when origin-host is configured as of “accept-inbound” connection type. If no inbound sockets are present these fields are not displayed.

- Inbound listening sockets
  - Local Host
  - Local Address
  - Endpoint
  - Task

CLI (Exec Mode)

show diameter peers [full | summary] [all | [endpoint *endpoint_name* **] [peer-host** *peer_id* **] [peer-realm** *realm_id* **]+] [| { grep** *grep_options* **| more }]**

Web Element Manager Path

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

show ims-authorization policy-control statistics

The output of this command includes the following new fields:

- DPCA Session Stats:
  - Total Secondary Create
  - Total Secondary Terminate
- DPCA Experimental Result Code Stats:
  - Error Initial Parameters
  - Error Trigger Event
  - Bearer Not Authorized
  - Traffic Mapping Rejected
  - PCC Rule Event
  - Base Result Code

CLI (Exec Mode)

show ims-authorization policy-control statistics

Web Element Manager Path

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

show ims-authorization sessions full

The output of this command includes the following new fields:

- Primary PCRF: The primary Policy Control and Charging Rules Function (PCRF) server host name.
- Secondary PCRF: The secondary PCRF server host name.
- Guaranteed Uplink Bw (in bps): The guaranteed bandwidth for uplink direction, in bps.
- Guaranteed Downlink Bw (in bps): The guaranteed bandwidth for downlink direction, in bps.

CLI (Exec Mode)

show ims-authorization session [full | summary] | [all | [ims-auth-service *ims_auth_svc_name* **| imsi** *imsi_value* **[nsapi** *nsapi_value* **] | apn** *apn_name* **| ip-address** *ip_address* **| callid** *call_id* **] [| { grep** *grep_options* **| more }]**

Web Element Manager Path

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

show resources

This command displays the resource information by CPU or session. In ACS Optimized mode, the output of this command displays the following ECS related fields:

- ECS Information:
  - Capacity
- Enhanced Charging Service:
  - In Use
  - Max Used
  - Limit
  - License Status

The output of this command for ACS Non-optimized mode remains unchanged.

CLI (Exec Mode)

show resources { cpu | session } [| { grep *grep_options* **| more }]**

Web Element Manager Path

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

show session subsystem facility sessmgr all

The output of this command includes the following new fields:

- aaa acct items (used/max)
- aaa buffer (used in MB/max in MB)
- Total aaa cancel auth
- Total aaa acct purged
- Total radius acct purged

CLI (Exec Mode)

`show session subsystem facility sessmgr all`

Web Element Manager Path

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

show subscribers

This command displays information for specified subscriber sessions. The **`nat`** keyword was added to this command. This enables viewing information for subscribers with NAT required or not required, as specified.

CLI (Exec Mode)

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

Web Element Manager Path

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

show subscribers full

This command displays information for specified subscriber sessions. The output of this command includes the following new fields:

- NAT Policy: Indicates whether Network Address Translation (NAT) is enabled for the subscriber.
- NAT Realm: The NAT realm associated with the subscriber.
- NAT IP address: The NAT IP address allocated from the NAT realm.

CLI (Exec Mode)

`show subscribers full`

Web Element Manager Path

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

Common Commands - Modified in Release 8.3

IMPORTANT

The commands documented in this section are only available in Release 8.3.

clear subscribers

The **nat-ip** filter keyword was added to this command. This optional filter keyword enables clearing information for subscribers with NAT processing enabled and using a specific NAT IP address.

CLI (Exec Mode)

clear subscribers [*keywords* **] [verbose] [-noconfirm] [| { grep** *grep_options* **| more }]**

Web Element Manager Path

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

show subscribers

The **nat-ip** filter keyword was added to this command. This optional filter keyword enables displaying information for subscribers with NAT processing enabled and using a specific NAT IP address.

CLI (Exec Mode)

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

Web Element Manager Path

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

show subscribers full

The output of this command includes the following new fields:

- Nat port chunks allocated [start - end]: Indicates the NAT port range allocated to the subscriber.
- Client Type: Displays the total number of subscriber sessions that have been labeled as data (data-only) or regular (includes voice).

CLI (Exec Mode)

show subscribers full

show subscribers full username

Web Element Manager Path

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

CF Commands - Modified in Release 8.0

The following CF commands were modified for Release 8.0.

show active-charging content-filtering category statistics

The **verbose** and **all** keywords were added to this command. The **all** keyword enables viewing content filtering category statistics for each configured rulebase in the active charging service separately. The **verbose** keyword displays detailed information.

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

This command displays information for Content Filtering Server Groups configured in the service. The output of this command includes the following new field:

- URL-extraction: Indicates the ICAP URL extraction mode.

CLI (Exec Mode)

show active-charging content-filtering server-group [statistics] [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

The optional keyword **facility srdbmgr [all | instance** *instance_value* **]** has been added to this command. This command displays the database statistics on the basis of running static rating database manager instances.

CLI (Exec Mode)

show content-filtering category database [active | all | facility srdbmgr [all | instance *instance_value* **] | url** *url_string* **] [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

The optional keyword **facility srdbmgr [all | instance** *instance_value* **]** has been added to this command. This command displays the content filtering category statistics on the basis of running static rating database manager instances.

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 statistics

The optional keyword **volume number** *volume_num* has been added to this command. This command displays the content filtering category statistics on the basis of category database volume.

CLI (Exec Mode)

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

Web Element Manager Path

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

CF Commands - Modified in Release 8.1

The following CF commands were modified for Release 8.1.

show active-charging content-filtering category policy-id

The output of this command includes the following new field:

- Reply Code: The reply code specified for www-reply-code-and-terminate-flow action.

CLI (Exec Mode)

show active-charging content-filtering category policy-id { all | id *policy_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 content-filtering category statistics verbose

The output of this command includes the following new fields:

- ALL (Default): Displays the number of URLs categorized by default action.
- Timeout: Displays the number of URLs categorized by time out action.
- x-category added during runtime, and the number of packets hit and blocked.

CLI (Exec Mode)

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

This command displays information for Content Filtering Server Groups configured in the service. The output of this command includes the following new field:

- URL-extraction: Indicates the ICAP URL extraction mode.

CLI (Exec Mode)

show active-charging content-filtering server-group [statistics] [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 active-charging service name

This command displays service and configuration counters for the all/specified active charging service. The output of this command now displays a description of the Content Filtering Policy ID, if set in the ACS Configuration Mode.

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 content-filtering category database

The output of this command has been modified to display the “Last Upgrade Status” field only once at top level, and not per database. The database status is also modified to display the database status as OK, loading, merging for optcmd.bin, optcmd_f.bin, and optcmd_i.bin depending on what function is being done on which database.

CLI (Exec Mode)

show content-filtering category database [active | all | facility srdbmgr [all | instance *instance_value* **] | url** *url_string* **] [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 policy-id

This command displays information about the Category-based Content Filtering application on the basis of policy identifier. The output of this command now includes the following:

- Discarded-Flow-Content-ID: Displays the content ID for the discarded flows. If not configured, this field is not displayed.
- A description of the Content Filtering Policy ID, if set in the ACS Configuration Mode.

CLI (Exec Mode)

show content-filtering category policy-id *cf_policy_id* **[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 instance

This command displays Category-based Content Filtering statistics. The output of this command now includes the following new field:

- x-category added during runtime, and the number of packets hit and blocked.

CLI (Exec Mode)

show content-filtering category statistics [all | facility srdbmgr [all | instance *instance_value* **] | volume number** *volume_num* **] [| { 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 8.0

The following ECS commands were modified in Release 8.0.

show active-charging analyzer statistics name ip verbose

The output of this command includes the following new fields:

- Uplink Bytes received after reassembly
- Uplink Pkts received after reassembly
- Downlink Bytes received after reassembly
- Downlink Pkts received after reassembly

CLI (Exec Mode)

show active-charging analyzer statistics name ip [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 charging-action name

The output of this command now includes the following field:

- Service ID

CLI (Exec Mode)

show active-charging charging-action { { { all | name *action_name* **} [service name** *svc_name* **] } | statistics [name** *action_name* **] } [| { grep** *grep_options* **| more }]**

Web Element Manager Path

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

show active-charging charging-action statistics

The output of this command includes the following new fields:

- Upl Pkts Readdressed
- Dnl Pkts Readdressed
- Upl Bytes Readdressed
- Dnl Bytes Readdressed

CLI (Exec Mode)

show active-charging charging-action { { { all | name *action_name* **} [service name** *svc_name* **] } | statistics [name** *action_name* **] } [| { grep** *grep_options* **| more }]**

Web Element Manager Path

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

show active-charging content-filtering server-group statistics

The output of this command includes the following new fields:

- Failure Action (communication with server-group not attempted):
  - Permit
  - Content Insertion
  - Discard
  - Terminate Flow
  - Redirect URL

CLI (Exec Mode)

show active-charging content-filtering server-group [statistics] [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 active-charging edr-udr-file statistics

The output of this command includes the following new fields:

- Overall Stats
  - Files rotated due to records limit
- EDR Specific Stats
  - EDR files rotated due to records limit
- UDR Specific Stats
  - UDR files rotated due to records limit

CLI (Exec Mode)

show active-charging edr-udr-file statistics

Web Element Manager Path

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

show active-charging ruledef

This command displays information for rule definitions configured in a service. The following changes were made to this command:

- The **firewall** keyword was added to this command.
- The **statistics** keyword options have changed to: "**statistics [all { charging | firewall [wide] } | name** *ruledef_name* **[wide]] }**".
- The "**service** *svc_name*" keyword is obsoleted.

CLI (Exec Mode)

show active-charging ruledef { all | charging | firewall | name *ruledef_name* **| routing | statistics [all { charging | firewall [wide] } | name** *ruledef_name* **[wide]] } [| { grep** *grep_options* **| more }]**

Web Element Manager Path

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

clear active-charging ruledef statistics

This command clears Active Charging rule definition statistics. The **charging** and **firewall** keywords were added to this command.

CLI (Exec Mode)

clear active-charging ruledef statistics [charging | firewall | name *ruledef_name* **] [| { grep** *grep_options* **| more }]**

Web Element Manager Path

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

show active-charging sessions

The **firewall { not-required | required }** filter was added to this command. This option displays information on sessions with firewall processing required or not required as specified.

CLI (Exec Mode)

show active-charging sessions [full | 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 sessions full

The output of this command includes the following new fields:

- NCQoS NRUPC Req Made
- NCQoS NRSPCA Req Made
- NCQoS NRUPC Req Failed
- NCQoS NRSPCA Req Failed
- NCQoS NRUPC Req Success
- NCQoS NRSPCA Req Success

CLI (Exec Mode)

show active-charging sessions [full | 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 sessions full all

The output of this command includes the following new fields:

- Current Readdressed Sessions
- Total Readdressed Uplink Pkts
- Total Readdressed Uplink Bytes
- Total Readdressed Downlink Pkts
- Total Readdressed Downlink Bytes

CLI (Exec Mode)

show active-charging sessions [full | 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 subsystem

The output of this command includes the following new fields:

- EDR/UDR statistics
  - Records Generated
  - Msgs sent to CDRMOD
  - Records sent to CDRMOD
  - Msgs bounced from CDRMOD
  - Records bounced from CDRMOD
  - Successful Msgs sent to CDRMOD
  - Successful records sent to CDRMOD

CLI (Exec Mode)

show active-charging subsystem all

Web Element Manager Path

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

show port info

The output of this command is now enhanced for Frame Relay interface and LMI protocol related following counters:

- Path x e1 y
- Frame Relay Intf Type
- Frame Relay LMI Type
- Frame Relay LMI n391
- Frame Relay LMI n392
- Frame Relay LMI n393

- Frame Relay LMI t391
- Frame Relay LMI t392
- Number of DLCIs

CLI (Exec Mode)

show port { **datalink counters** [*slot/port*] | **info** [*slot/port*] | **npu counters** [*slot/port* [**tagged** | **untagged** | **vlan** *tag_id*]] | **table** | **utilization table** } [**|** { **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 8.1

IMPORTANT

The following ECS commands were modified in Release 8.1.

clear active-charging analyzer statistics

This command is used to clear protocol analyzer statistics. The following P2P application protocol options were added to this command:

- ddlink
- halflife2
- hamachivpn
- irc
- oscar
- popo
- steam
- tvants
- tvuplayer
- uusee
- vpnx
- vtun
- winmx
- wofwarcraft
- xbox

CLI (Exec Mode)

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

Web Element Manager Path

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

clear active-charging credit-control statistics

This command clears prepaid credit control service statistics in an Active Charging Service. The **`group`** keyword was added to this command. This enables clearing statistics for a specific credit control group.

CLI (Exec Mode)

`clear active-charging credit-control statistics [ group` *`group_name`* **`]`**

Web Element Manager Path

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

show active-charging analyzer statistics name p2p

The output of this command includes the following new fields:

- Ddlink
- Halflife2
- Hamachivpn
- Irc
- Oscar
- Popo
- Steam
- Tvants
- Tvuplayer
- Uusee
- Vpnx
- Vtun
- Winmx
- Wofwarcraft
- Xbox

CLI (Exec Mode)

show active-charging analyzer statistics name p2p

Web Element Manager Path

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

show active-charging charging-action all

The output of this command includes the following new fields:

- Billing Action:
  - Event Data Record: Indicates whether EDRs are enabled/disabled.
  - GGSN charging Data Record: Indicates whether GGSN CDRs are enabled/disabled.
  - User Data Record: Indicates whether UDRs are enabled/disabled.
  - Radius Accounting Record: Indicates whether RADIUS accounting records is enabled/disabled.

CLI (Exec Mode)

show active-charging charging-action { { { all | name *action_name* **} [service name** *svc_name* **] } | statistics [name** *action_name* **] } [| { grep** *grep_options* **| more }]**

Web Element Manager Path

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

show active-charging credit-control statistics

This command displays statistics for Diameter/RADIUS prepaid credit control service in an Active Charging Service. The **group** keyword was added to this command. This enables viewing statistics for a specific credit control group. If credit control group(s) are configured, the output of this command will display statistics per credit control group.

CLI (Exec Mode)

show active-charging credit-control { statistics [all | group *group_name* **] | session-states [rulebase** *rulebase_name* **] [content-id** *content_id* **] } [| { grep** *grep_options* **| more }]**

Web Element Manager Path

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

show active-charging flows

This command displays active charging flows in a system or service. The following P2P application protocol options were added to this command:

- ddlink
- halflife2
- hamachivpn
- irc
- oscar
- popo
- steam
- tvants
- tvuplayer
- uusee
- vpnx
- vtun
- winmx
- wofwarcraft
- xbox

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* **] [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 flows full

This command displays active charging flows in a system or service. The output of this command includes the following new fields:

- MS NAT IP: The NAT IP address used by the subscriber flow.
- TCP MS NAT Port: The NAT port number used by the subscriber flow. This field is not displayed for one-to-one NAT.

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* **] [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 name

The output of this command includes the following new fields:

- Flow Any Error Charging Action: Indicates the charging action configured for action on packets dropped by Firewall due to any error. If disabled, no accounting is performed on such packets.
- Type: Indicates the Firewall rule definition type.
- Firewall Configuration:
- Dos-Protection:
  - Source-Route: Indicates status of protection against IP Source Route IP Option attacks.
  - Win-Nuke: Indicates status of protection against Win Nuke attacks.
  - Mime-Flood: Indicates status of protection against MIME Flood attacks.
  - FTP-Bounce: Indicates status of protection against FTP Bounce attacks.
  - IP-Unaligned-Timestamp: Indicates status of protection against IP Unaligned Timestamp attacks.
  - Seq-Number-Prediction: Indicates status of protection against Sequence Number Prediction attacks.
  - TCP-Window-Containment: Indicates status of protection against TCP Window Containment.
  - Teardrop: Indicates status of protection against Teardrop attacks.

  - UDP Flooding: Indicates status of protection against UDP Flooding attacks.
  - ICMP Flooding: Indicates status of protection against ICMP Flooding attacks.
  - SYN Flooding: Indicates status of protection against SYN Flooding attacks.
  - Port Scan: Indicates status of protection against Port Scan attacks.
- Flooding:
  - ICMP limit: The maximum number of ICMP packets allowed during a sampling interval.
  - UDP limit: The maximum number of UDP packets allowed during a sampling interval.
  - TCP-SYN limit: The maximum number of TCP-SYN packets allowed during a sampling interval.
  - Sampling Interval: The flooding sampling interval, in seconds.
- TCP-SYN Flood Intercept:
  - Mode: The TCP SYN flood intercept mode.
  - Max-Attempts: The maximum number of attempts for sending proxy SYN to the target.
  - Retrans-timeout: The SYN-Proxy retransmit timeout, in seconds.
  - Watch-timeout: The TCP intercept watch timeout, in seconds.
- Mime-Flood Params:
  - HTTP Header-Limit: The maximum number of headers allowed in an HTTP packet.
  - HTTP Max-Header-Field-Size: The maximum header field size allowed in an HTTP header, in bytes.
- URL-Blacklisting Action: Indicates action to be taken on URL Blacklisting match.
- URL-Blacklisting EDR: Indicates whether EDRs will be generated on Blacklisting match.
- Content Filtering Flow Any Error: Indicates whether Content Filtering packets are allowed/discarded in case of ACS error scenarios.
- Content-Filtering: Indicates whether EDRs are generated for Content Filtering.
- Charging Action Priorities:
  - Timedef: Indicates the time definition configured with the ruledef / group-of-ruledefs.

CLI (Exec Mode)

show active-charging rulebase { all [service name *svc_name* **] | name** *rulebase_name* **[service name** *svc_name* **] | 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 rulebase statistics

The output of this command includes the following new fields:

- R7Gx Rule-Matching Failure Stats:
  - Total Dropped Packets
  - Total Dropped Packet Bytes
  - TCP MSS Inserted Pkts
  - TCP MSS Limited Pkts
- EDRs:
  - EDRs generated for any-error packets
  - EDRs generated for flow-end content-filtering
  - EDRs generated for firewall deny rule match
  - EDRs generated for transaction completion

CLI (Exec Mode)

show active-charging rulebase { all [service *svc_name* **] \| name** *rulebase_name* **[service** *svc_name* **] \| 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 service

The output of this command includes the following new fields:

- Content Filtering: Indicates whether active-charging category-based content-filtering is enabled.
- URL-Blacklisting: Indicates whether URL Blacklisting is enabled.
- URL-Blacklisting Match-method: Indicates the URL Blacklisting match method to look up URLs in the URL Blacklisting database.
- Content Filtering Match-method: Indicates the match method to look up URLs in the category-based content filtering database.

The following fields were removed from the output of this command:

- Content Filtering Policy
- Content Filtering Categories
  - Category
  - Priority
  - Action
  - Content Insert
  - Redirect
- EDR
- Timeout Action

CLI (Exec Mode)

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

Web Element Manager Path

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

show active-charging sessions

This command displays statistics for specific active charging service sessions. The following keywords were added to this command:

- The following P2P application protocol options were added to this command:
  - ddlink
  - halflife2
  - hamachivpn
  - irc
  - oscar
  - popo
  - steam
  - tvants
  - tvuplayer
  - uusee
  - vpnx
  - vtun
  - winmx
  - wofwarcraft
  - xbox
- The **nat** keyword was added to this command. This enables viewing session information for sessions with Network Address Translation required or not required, as specified.

CLI (Exec Mode)

show active-charging sessions [full | 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 sessions

This command displays statistics for specific active charging service sessions. The output of this command includes the following new fields:

- Current DDLINK Sessions
- Current HALFLIFE2 Sessions
- Current HAMACHIVPN Sessions
- Current IRC Sessions
- Current OSCAR Sessions
- Current POPO Sessions
- Current STEAM Sessions
- Current TVANTS Sessions
- Current TVUPLAYER Sessions
- Current UUSEE Sessions
- Current VPNX Sessions
- Current VTUN Sessions
- Current WINMX Sessions
- Current WOFWARCRAFT Sessions
- Current XBOX Sessions
- Predefined Firewall Rules Enabled List
- R7Gx Dropped Upl Pkts RuleMatch Fail
- R7Gx Dropped Upl Bytes RuleMatch Fail
- R7Gx Dropped Dnl Pkts RuleMatch Fail
- R7Gx Dropped Dnl Bytes RuleMatch Fail

CLI (Exec Mode)

show active-charging sessions [full | 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 subsystem

The output of this command includes the following new fields:

- Session Creation Succ
- Session Creation Fail
- Total Flows Connected
- Total Flows Disconnected
- Total Uplink Pkts
- Total Uplink Bytes
- Total Downlink Pkts
- Total Downlink Bytes
- Total Rule-Hits
- Total Blacklisted URL hits
- Total Blacklisted URL misses
- Total P2P Voice flows
- Current P2P Voice flows

CLI (Exec Mode)

`show active-charging subsystem all`

Web Element Manager Path

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

show active-charging subsystem facility acsmgr instance

The output of this command includes the following new fields:

- Total Blacklisted URL hits
- Total Blacklisted URL misses

CLI (Exec Mode)

`show active-charging subsystem facility acsmgr instance` *`instance_value`*

Web Element Manager Path

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

ECS Commands - Modified in Release 8.3

IMPORTANT

The following ECS commands were modified in Release 8.3.

show active-charging edr-format statistics

The output of this command includes the following new field:

- Total NAT bind records generated

CLI (Exec Mode)

show active-charging edr-format statistics

Web Element Manager Path

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

show active-charging charging-action statistics name

The output of this command includes the following new fields:

- PP Upl Pkts Readdressed
- PP Dnl Pkts Readdressed
- PP Upl Bytes Readdressed
- PP Dnl Bytes Readdressed
- pp-flow-action

The following fields were modified:

- Statistic
- flow-action
- pp-flow-action
- flow-limit
- bandwidth-limit

CLI (Exec Mode)

show active-charging charging-action statistics name *charging_action_name* **[service-name** *service_name* **] [| { grep** *grep_options* **| more }]**

Web Element Manager Path

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

show active-charging flows

The **nat** filter keyword was added to this command. This optional keyword enables displaying information for flows with NAT processing disabled or enabled and optionally using a specific NAT IP address or a specific NAT IP address and NAT port number.

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 ruledef

The following changes were made to this command:

- The **post-processing** keyword was added to this command. This enables to view post-processing ruledef related information.
- Output of the **show active-charging ruledef statistics** command includes the following new fields:
  - Total Post-processing Ruledefs
  - Uplink Packets
  - Uplink Bytes
  - Downlink Packets
  - Downlink Bytes
  - Hits

CLI (Exec Mode)

show active-charging ruledef { all | charging | firewall | name *ruledef_name* **| post-processing | routing | statistics [all { charging | firewall [wide] | post-processing } | name** *ruledef_name* **[wide]] } [| { 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 name

The output of this command includes the following new fields:

- Post-processing Action Priorities:
  - Name
  - Type
  - Priority
  - Charging-action
  - Description

CLI (Exec Mode)

show active-charging rulebase name *rulebase_name* **service name** *service_name* **[| { grep** *grep_options* **| more }]**

Web Element Manager Path

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

show active-charging rulebase statistics

The output of this command includes the following new field:

- NBRs:
  - Total NBRs generated
  - NBRs generated for port chunk allocation
  - NBRs generated for port chunk release

CLI (Exec Mode)

show active-charging rulebase statistics

Web Element Manager Path

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

show active-charging rulebase statistics name

The output of this command includes the following new fields:

- Total PP Dropped Packets
- Total PP Dropped Packet Bytes

CLI (Exec Mode)

show active-charging rulebase statistics name *rulebase_name* **[| { grep** *grep_options* **| more }]**

show active-charging sessions full all

The output of this command includes the following new field:

- PP Flow action Terminated Flows

CLI (Exec Mode)

show active-charging sessions full all [| { grep *grep_options* **| more }]**

Web Element Manager Path

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

show active-charging subsystem all

The output of this command includes the following new field:

- Total PP Rule-Hits

CLI (Exec Mode)

show active-charging subsystem all [rulebase 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 8.1

The following Firewall commands were modified in Release 8.1.

clear active-charging firewall statistics

This command clears Active Charging Stateful Firewall statistics. The **nat-realm** keyword was added to this command. This enables clearing NAT realm statistics.

CLI (Exec Mode)

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

Web Element Manager Path

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

show active-charging firewall statistics

This command displays Active Charging Stateful Firewall statistics. The **nat-realm** keyword was added to this command. This enables viewing NAT realm statistics.

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 8.0

The following GGSN commands were modified in Release 8.0.

show apn statistics name

The output of this command enhanced and modified to include statistics for traffic policing and shaping:

CLI (Exec Mode)

show apn statistics [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 gtpc full

The output of this command now includes the following counters for direct tunnel support:

- GTP-U Tunnel Establishment

CLI (Exec Mode)

show gtpc [full | counters | summary] { all | apn *apn_name* **| imsi** *imsi_value* **[nsapi** *nsapi_value* **] | callid** *callid* **| sgsn-address** *ip_address* **| ggsn-service** *ggsn_name* **| user-address** *ip_address* **| username** *username* **}**

Web Element Manager Path

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

show gtpc statistics verbose

The output of this command now includes the following counters for direct tunnel support:

- GTP-U Tunnel Establishment with RNC
- Direct Tunnels Established
- Direct Tunnels torn down by SGSNs
- Direct Tunnels that received Error Indication
- Direct Tunnel Flags update

CLI (Exec Mode)

show gtpc statistics [sgsn-address *ip_address* **| ggsn-service** *ggsn_name* **| apn-name** *apn_name* **] [verbose]**

Web Element Manager Path

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

show gtpc statistics verbose

The output of this command includes the following new fields:

- Update PDP Tx Reasons
- QoS Change
- Providing PDP address
- APN Restriction
  - No APN Subscription
- Local IP Pool All Address Occupied

CLI (Exec Mode)

```
show gtpc statistics verbose
```

Web Element Manager Path

Click Performance | GGSN | GTPC Statistics.

show gtpp counters all

The output of this command now includes the following counters:

- Outstanding G-CDRs
- Possibly Duplicate Outstanding G-CDRs
- Archived G-CDRs
- G-CDRs buffered with AAAPROXY
- G-CDRs buffered with AAAMGR

CLI (Exec Mode)

```
show gtpp counter all
```

Web Element Manager Path

Click Performance | GGSN | GTPP Statistics.

show gtpp statistics cgf-address

The output of this command includes the following new fields:

- CDR Decode Error
- Seq No incorrect
- Unknown Cause

CLI (Exec Mode)

```
show gtpp statistics cgf-address
```

Web Element Manager Path

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

GGSN Commands - Modified in Release 8.1

show gtpp storage-server

A new keyword has been added to this command to display statistics and counter for files stored on the SMC hard disk.

CLI (Exec Mode)

`show gtpp storage-server local file { counters | statistics }`

Web Element Manager Path

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

show subscriber ggsn-only

New counter has been added to display the applicable IP allocation method for MBMS session for GGSN subscribers. Added counter is:

- ip-type-unknown

CLI (Exec Mode)

`show subscribers ggsn-only [ | { grep` *`grep_options`* **`| more } ]`**

Web Element Manager Path

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

show apn name

Output of this command is modified for new counters for Bearer Control mode information and also irrelevant counters are removed from screen output of this command.

Counters removed:

- ip vlan id
- eap msk lifetime
- rohc-profile-name
- compression mode
- data compression size
- min compression size
- dns-proxy-intercept-list

Counter Added:

- Bearer Control Mode

CLI (Exec Mode)

`show apn { 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 subscribers

The output of this command is enhanced to display following counters with **ggsn-only** or other GGSN-specific filter keywords:

- in packet dropped due to zero mbr
- out packet dropped due to zero mbr

CLI (Exec Mode)

show subscribers
show subscribers full
show subscribers full username
show subscribers counters username
show subscribers ggsn-only full
show subscribers summary
show subscribers ggsn-only summary

Web Element Manager Path

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

show gtpc statistics

New keyword **custom1** added to this command to display GTP-C statistics and counters for Preservation Mode and Free-of-Charge service. This is a customer-specific feature.

CLI (Exec Mode)

show gtpc statistics [apn-name *apn_name* **] [custom1] [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.

clear gtpc statistics

New keyword **custom1** added to this command to clear the GTP-C statistics and counters for Preservation Mode and Free-of-Charge service. This is a customer-specific feature.

CLI (Exec Mode)

clear gtpc statistics [apn-name *apn_name* **] [custom1] [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.

show apn statistics

Following counters has been added to the output of this command to indicate the auto readjusted dynamic burst size for guaranteed and peak burst size under traffic shaping feature:

- Burst Size
- Auto Readjust
- Auto Readjust Duration

- Peak Burst Size (bytes)
- Guaranteed Burst Size (bytes)

CLI (Exec Mode)

show apn statistics [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 apn all

Following counters has been added to the output of this command to indicate the auto readjusted dynamic burst size for guaranteed and peak burst size under traffic shaping feature:

- Burst Size
- Auto Readjust
- Auto Readjust Duration
- Peak Burst Size (bytes)
- Guaranteed Burst Size (bytes)

CLI (Exec Mode)

show apn { 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 subscribers ggsn-only

Following counters has been added to the output of this command to indicate the auto readjusted dynamic burst size for guaranteed and peak burst size under traffic shaping feature:

- Downlink traffic-rate-limit
- Uplink traffic-rate-limit
- Downlink traffic-shaping
- Uplink traffic-shaping
- Burst Size
- Auto Readjust
- Auto Readjust Duration
- Peak Burst Size (bytes)
- Guaranteed Burst Size (bytes)
- Peak data rate (bps)
- Guaranteed data rate (bps)

CLI (Exec Mode)

show subscribers ggsn-only [| { grep *grep_options* **| more }]**

Web Element Manager Path

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

HA Commands - Modified in Release 8.0

There were no HA commands modified in Release 8.0.

HA Commands - Modified in Release 8.1

There were no HA commands modified in Release 8.1.

PDIF Commands - Modified in Release 8.0

PDIF is not supported in Release 8.0.

PDIF Commands - Modified in Release 8.1

show crypto statistics ikev2

This command has been modified to show the number of internal failure messages sent to the peer after an internal failure in ipsecmgr or dcardmgr.

CLI (Exec Mode)

`show crypto statistics ikev2`

Web Element Manager Path

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

show crypto managers instance

This command has been modified to show the number of internal failure messages sent to the peer after an internal failure in ipsecmgr or dcardmgr.

CLI (Exec Mode)

`show crypto managers instance <`*`instance number`***`>`**

Web Element Manager Path

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

show crypto map

This command has been modified with the keyword **`ikev2-pdif`**. Now instead of seeing all created transform-sets without knowing which is in use, the new command returns only two: the one that created the IKE SA and the one that created the IPSec SA.

CLI (Exec Mode)

show crypto map map-type ikev2-pdif

Web Element Manager Path

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

This command has been modified with the keyword **`summary`**. This new option displays summary information for all crypto maps configured in the context.

CLI (Exec Mode)

show crypto map summary

Web Element Manager Path

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

show session subsystem facility aaamgr all

The output of this command includes the following new fields:

- aaa request (used/max)
- Total Diameter auth requests
- Current Diameter auth requests
- Total Diameter auth requests retried
- Total Diameter auth requests dropped
- Total radius auth responses dropped
- Total Diameter acct requests
- Current Diameter acct requests
- Total Diameter auth acct requests retried
- Total radius acct cancelled
- total radius acct purged
- total radius acct responses dropped
- Total aaamgr purged requests

CLI (Exec Mode)

`show session subsystem facility aaamgr`

Web Element Manager Path

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

show crypto ipsec security-associations

This command has been modified to indicate whether rekeying is enabled.

CLI (Exec Mode)

show crypto ipsec security associations

Web Element Manager Path

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

This command has been modified to display the SA State and Crypto Type.

CLI (Exec Mode)

show crypto ipsec security associations

Web Element Manager Path

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

PDIF Commands - Modified in Release 8.3

show crypto transform-set

This command has been modified in PDIF Release 8.3 to include the ipsec keyword for clarity. It does not change the command output.

CLI (Exec Mode)

Previous command syntax:

```
show crypto transform-set
```

Modified command syntax:

```
show crypto ipsec transform-set
```

Web Element Manager Path

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

show pdif-service statistics

This command has been modified in PDIF Release 8.3 to include the Total Pkts Violations field in the command output. This field lists the total number of packets received from UEs and destined for the Internet that do not match any of the configured traffic selectors.

CLI (Exec Mode)

```
show pdif-service statistics
show pdif-service statistics peer-address
```

Web Element Manager Path

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

PDSN Commands - Modified in Release 8.0

There were no PDSN commands modified in Release 8.0.

PDSN Commands - Modified in Release 8.1

show hd raid verbose

New fields have been added to the output for this command. When two SMCs contain different disk images, a user who wants to decide which disk to use needs the create/update time and event counts information.

CLI (Exec Mode)

`show hd raid verbose`

Web Element Manager Path

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

Session Control Manager Commands - Modified for Release 8.0

Session Control Manager is not supported in Release 8.0.

Session Control Manager Commands - Modified for Release 8.1

The following commands have been modified in Release 8.1.

clear cscf service

This command was changed in synch with the associated show command.

CLI (Exec Mode)

clear cscf service { diameter policy_control statistics [service-name *service_name* **| vpn-name** *name* **] | li-packet-cable statistics | statistics name** *service_name* **{ all | calls | ip-security | message | package-name { message-summary | presence | reg | winfo } | registrations | sigcomp | tcp | vpn-name** *name* **} }**

Web Element Manager Path

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

clear cscf sessions

This command was changed in synch with the associated show command.

CLI (Exec Mode)

clear cscf sessions { counters { calls | subscription } service *service_name* **| service** *service_name* **{ all | session-id** *id* **| aor** *aor* **}**

Web Element Manager Path

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

clear cscf sip

This command was changed in synch with the associated show command.

CLI (Exec Mode)

clear cscf sip statistics [name *service_name* **[interface { domain name** *domain_name* **| ip address** *ip_address* **} | vpn-name** *name* **]**

Web Element Manager Path

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

show cscf service

This command was expanded to allow more options.

CLI (Exec Mode)

show cscf service { all [counters] | diameter policy_control statistics service-name *service_name* **[vpn-name** *name* **] | grey-list name** *name* **| li-packet-cable statistics | name** *service_name* **[counters] | statistics name** *service_name* **[all | calls | ip-security | message | package-name { message-summary | presence | reg | winfo } | registrations | sigcomp | tcp | vpn-name** *name* **] | subscription name** *service_name* **} [| { grep** *grep_options* **| more }]**

Web Element Manager Path

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

show cscf sessions

This command was expanded to allow more options.

CLI (Exec Mode)

show cscf sessions { counters { calls { duration | first-response-time | invite-processing-time | post-answer-delay | post-dial-delay | service *service_name* **| session-release-delay | session-setup-delay } service** *service_name* **| subscription { duration | service service_name | setup-time} service** *service_name* **} | duration | full [callleg-id** *id* **| from-aor** *aor* **| service service_name | session-id id | to-aor aor] [media-type type] | summary [from-aor** *aor* **| service** *service_name* **| session-id** *id* **| to-aor** *aor* **] } [| { grep grep_options | more }]**

Web Element Manager Path

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

show cscf sip

This command has a new keyword - **interface**.

CLI (Exec Mode)

show cscf sip statistics name *service_name* **[interface { domain** *domain_name* **| ip address** *ip_address* **} | vpn-name** *name* **] [| { grep grep_options | more }]**

Web Element Manager Path

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

show cscf tcp connections

This **facility**, **remote-ip**, and **remote-port** keywords have been added to specify SIP interfaces.

CLI (Exec Mode)

show cscf tcp connections service service_name [facility { cscfmgr | sessmgr } | full | remote-ip *ip_address* **| remote-port** *port_number* **] [| { grep grep_options | more }]**

Web Element Manager Path

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

SGSN Commands - Modified in Release 8.0

The following SGSN commands were modified in Release 8.0.

show dns-client

The output of this command is now enhanced for SGSN specific counters to show DNS cache statistics with the following counters:

- DNS Cache Statistics
- Central Cache
- Local Cache
- Total Lookups
- Cache Hits (Positive Response)
- Cache Hits (Negative Response)
- Not Found in Cache
- Hit Ratio (Percentage)
- DNS Resolver Statistics
- Successful Queries
- Query Timeouts
- Domain Not Found
- Connection Refused
- Other Failures

CLI (Exec Mode)

show dns-client *name* { cache [query-name *name* | query-type
{ A | SRV }] | statistics }

Web Element Manager Path

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

show gmm-sm statistics

This command has a new keyword - routing-area - which enables fine tuning the statistics display to a specified routing area.

CLI (Exec Mode)

show gmm-sm statistics [gmm-only | sm-only] [gprs-service *srvc_name* **[nsei** *nse_id* **| routing-area mcc** *mc_code* **mnc** *mn_code* **lac** *loc_code* **rac** *ra_code* **]] | [sgsn-service** *srvc_name* **[rnc mcc** *mc_code* **mnc** *mn_code* **rnc-id** *rnc_id* **| routing area mcc** *mc_code* **mnc** *mn_code* **lac** *loc_code* **rac** *ra_code* **]] [verbose] [| { grep** *grep_options* **| more }]**

Web Element Manager Path

Configuration of these features is not yet supported by the Web Element Manager.

show gmm-sm statistics

This command is enhanced with new keywords for RNC related statistics and output of this command is also enhanced for RNC related statistics.

CLI (Exec Mode)

show gmm-sm statistics { gmm-only [gprs-service *srvc_name* **] | gprs-service** *srvc_name* **| sgsn-service** *srvc_name* **[rnc mcc** *mc_code* **mnc** *mn_code* **rnc-id** *rnc_id* **| routing area mcc** *mc_code* **mnc** *mn_code* **lac** *loc_code* **rac** *ra_code* **] | sm-only [gprs-service** *srvc_name* **] } [verbose] [| { grep** *grep_options* **| more }]**

Web Element Manager Path

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

show gmm-sm statistics

Several new counters have been added under the heading of Network Overload Protection:

- Attach requests queued in the pacing queue:
- Inter SGSN RAU requests queued in the pacing queue:
- Number of Inter SGSN RAU and Attach requests in the pacing queue:
- Attach requests successfully dequeued from the pacing queue:
- Inter SGSN RAU requests successfully dequeued from the pacing queue:
- Attaches rejected:
- Inter SGSN RAUs rejected:
- Attaches dropped:
- Inter SGSN RAUs dropped:

CLI (Exec Mode)

show gmm-sm statistics [verbose]

show gmm-sm statistics

The SGSN GMM-SM statistics now supports counters for inter-rat / inter-service for RAU/Attaches. Previously, RAU (requests/accepts/rejects) statistics display counters were classified under 5 categories:

1.Intra-sgsn periodic rau
2.Intra-sgsn gprs-only rau
3.Intra-sgsn combined rau
4.Inter-sgsn periodic rau
5.Inter-sgsn combined rau

The following categories have been added:

6.Intra-sgsn Inter-rat gprs-only rau
7.Intra-sgsn Inter-rat combined rau
8.Intra-sgsn Intra-rat Inter-service gprs-only rau
9.Intra-sgsn Intra-rat Inter-service combined rau

The statistics for these categories, relate as follows:

(4 & 5) -> RAU from completely different sgsn
(6 & 7) -> RAU between sgsn-service <-> gprs-service
(8 & 9) -> RAU between 2 sgsn-services or 2 gprs-services.

A large range of counters have been added within the new categories:

Routing Area Update Request:

- Total-Ps-Inter-Rat-RAU
  - 3G-Ps-Inter-Rat-RAU
  - 2G-Ps-Inter-Rat-RAU
- Total-Comb-Inter-Rat-RAU
  - 3G-Comb-Inter-Rat-RAU
  - 2G-Comb-Inter-Rat-RAU
- Total-Ps-Inter-Serv-RAU
  - 3G-Ps-Inter-Serv-RAU
  - 2G-Ps-Inter-Serv-RAU 0
- Total-Comb-Inter-Serv-RAU
  - 3G-Comb-Inter-Serv-RAU
  - 2G-Comb-Inter-Serv-RAU
- Ret-Total-Ps-Inter-Rat-RAU
  - Ret-3G-Ps-Inter-Rat-RAU
  - Ret-2G-Ps-Inter-Rat-RAU
- Ret-Total-Comb-Inter-Rat-RAU
  - Ret-3G-Comb-Inter-Rat-RAU
  - Ret-2G-Comb-Inter-Rat-RAU
- Ret-Total-Ps-Inter-Serv-RAU
  - Ret-3G-Ps-Inter-Serv-RAU
  - Ret-2G-Ps-Inter-Serv-RAU
- Ret-Total-Comb-Inter-Serv-RAU
  - Ret-3G-Comb-Inter-Serv-RAU
  - Ret-2G-Comb-Inter-Serv-RAU

Routing Area Update Accept:

- Total-Ps-Inter-Rat-RAU-Acc
  - 3G-Ps-Inter-Rat-RAU-Acc
  - 2G-Ps-Inter-Rat-Acc
- Total-Comb-Inter-Rat-RAU-Acc
  - 3G-Comb-Inter-Rat-RAU-Acc
  - 2G-Comb-Inter-Rat-Acc
- Total-Ps-Inter-Serv-RAU-Acc

    - 3G-Ps-Inter-Serv-RAU-Acc
    - 2G-Ps-Inter-Serv-RAU-Acc
- Total-Comb-Inter-Serv-RAU-Acc
    - 3G-Comb-Inter-Serv-RAU-Acc
    - 2G-Comb-Inter-Serv-RAU-Acc
- Ret-Total-Ps-Inter-Rat-RAU-Acc
    - Ret-3G-Ps-Inter-Rat-RAU-Acc
    - Ret-2G-Ps-Inter-Rat-Acc
- Ret-Total-Comb-Inter-Rat-RAU-Acc
    - Ret-3G-Comb-Inter-Rat-RAU-Acc
    - Ret-2G-Comb-Inter-Rat-Acc
- Ret-Total-Ps-Inter-Serv-RAU-Acc
    - Ret-3G-Ps-Inter-Serv-RAU-Acc
    - Ret-2G-Ps-Inter-Serv-RAU-Acc
- Ret-Total-Comb-Inter-Serv-RAU-Acc
    - Ret-3G-Comb-Inter-Serv-RAU-Acc
    - Ret-2G-Comb-Inter-Serv-RAU-Acc

Routing Area Update Reject:

- Inter RAT PS Only Routing Area Update Reject Causes:
    - 3G-IMSI Unknown in HLR
    - 2G-IMSI Unknown in HLR
    - 3G-Illegal MS
    - 2G-Illegal MS
    - 3G-Illegal ME
    - 2G-Illegal ME
    - 3G-GPRS service not allowed
    - 2G-GPRS service not allowed
    - 3G-GPRS and Non-GPRS service not allowed
    - 2G-GPRS and Non-GPRS service not allowed
    - 3G-MsId not derived by Nw
    - 2G-MsId not derived by Nw
    - 3G-Implicitly Detached
    - 2G-Implicitly Detached
    - 3G-PLMN not allowed
    - 2G-PLMN not allowed
    - 3G-Location Area not allowed
    - 2G-Location Area not allowed
    - 3G-Roaming not allowed in this Location Area

- 2G-Roaming not allowed in this Location Area
- 3G-GPRS service not allowed in this PLMN
- 2G-GPRS service not allowed in this PLMN
- 3G-No suitable cells in this Location Area
- 2G-No suitable cells in this Location Area
- 3G-MSC not reachable
- 2G-MSC not reachable
- 3G-Network Failure
- 2G-Network Failure
- 3G-MAC Failure
- 2G-MAC Failure
- 3G-SYNC Failure
- 2G-SYNC Failure
- 3G-Congestion
- 2G-Congestion
- 3G-GSM Auth Unacceptable
- 2G-GSM Auth Unacceptable
- 3G-No PDP contexts activated
- 2G-No PDP contexts activated
- 3G-Retry from new cell
- 2G-Retry from new cell
- 3G-Semantically Wrong Msg
- 2G-Semantically Wrg Msg
- 3G-Invalid Mandatory Info
- 2G-Invalid Mandatory Info
- 3G-MSG type Non Existent
- 2G-MSG type Non Existent
- 3G-MSG type not compatible with protocol state
- 2G-MSG type not compatible with protocol state
- 3G-IE Non Existent
- 2G-IE Non Existent
- 3G-Conditional IE Error
- 2G-Conditional IE Error
- 3G-Message not compatible with protocol state
- 2G-Message not compatible with protocol state
- 3G-Protocol Error
- 2G-Protocol Error
- 3G-Unknown cause

- 2G-Unknown cause

- Inter RAT Comb. Routing Area Update Reject Causes:
  - 3G-IMSI Unknown in HLR
  - 2G-IMSI Unknown in HLR
  - 3G-Illegal MS
  - 2G-Illegal MS
  - 3G-Illegal ME
  - 2G-Illegal ME
  - 3G-GPRS service not allowed
  - 2G-GPRS service not allowed
  - 3G-GPRS and Non-GPRS service not allowed
  - 2G-GPRS and Non-GPRS service not allowed
  - 3G-MsId not derived by Nw
  - 2G-MsId not derived by Nw
  - 3G-Implicitly Detached
  - 2G-Implicitly Detached
  - 3G-PLMN not allowed
  - 2G-PLMN not allowed
  - 3G-Location Area not allowed
  - 2G-Location Area not allowed
  - 3G-Roaming not allowed in this Location Area
  - 2G-Roaming not allowed in this Location Area
  - 3G-GPRS service not allowed in this PLMN
  - 2G-GPRS service not allowed in this PLMN
  - 3G-No suitable cells in this Location Area
  - 2G-No suitable cells in this Location Area
  - 3G-MSC not reachable
  - 2G-MSC not reachable
  - 3G-Network Failure
  - 2G-Network Failure
  - 3G-MAC Failure
  - 2G-MAC Failure
  - 3G-SYNC Failure
  - 2G-SYNC Failure
  - 3G-Congestion
  - 2G-Congestion
  - 3G-GSM Auth Unacceptable
  - 2G-GSM Auth Unacceptable

- 3G-No PDP contexts activated
- 2G-No PDP contexts activated
- 3G-Retry from new cell
- 2G-Retry from new cell
- 3G-Semantically Wrong Msg
- 2G-Semantically Wrg Msg
- 3G-Invalid Mandatory Info
- 2G-Invalid Mandatory Info
- 3G-MSG type Non Existent
- 2G-MSG type Non Existent
- 3G-MSG type not compatible with protocol state
- 2G-MSG type not compatible with protocol state
- 3G-IE Non Existent
- 2G-IE Non Existent
- 3G-Conditional IE Error
- 2G-Conditional IE Error
- 3G-Message not compatible with protocol state
- 2G-Message not compatible with protocol state
- 3G-Protocol Error
- 2G-Protocol Error
- 3G-Unknown cause
- 2G-Unknown cause

- Inter Service PS Only Routing Area Update Reject Causes:
  - 3G-IMSI Unknown in HLR
  - 2G-IMSI Unknown in HLR
  - 3G-Illegal MS
  - 2G-Illegal MS
  - 3G-Illegal ME
  - 2G-Illegal ME
  - 3G-GPRS service not allowed
  - 2G-GPRS service not allowed
  - 3G-GPRS and Non-GPRS service not allowed
  - 2G-GPRS and Non-GPRS service not allowed
  - 3G-MsId not derived by Nw
  - 2G-MsId not derived by Nw
  - 3G-Implicitly Detached
  - 2G-Implicitly Detached
  - 3G-PLMN not allowed

- 2G-PLMN not allowed
- 3G-Location Area not allowed
- 2G-Location Area not allowed
- 3G-Roaming not allowed in this Location Area
- 2G-Roaming not allowed in this Location Area
- 3G-GPRS service not allowed in this PLMN
- 2G-GPRS service not allowed in this PLMN
- 3G-No suitable cells in this Location Area
- 2G-No suitable cells in this Location Area
- 3G-MSC not reachable
- 2G-MSC not reachable
- 3G-Network Failure
- 2G-Network Failure
- 3G-MAC Failure
- 2G-MAC Failure
- 3G-SYNC Failure
- 2G-SYNC Failure
- 3G-Congestion
- 2G-Congestion
- 3G-GSM Auth Unacceptable
- 2G-GSM Auth Unacceptable
- 3G-No PDP contexts activated
- 2G-No PDP contexts activated
- 3G-Retry from new cell
- 2G-Retry from new cell
- 3G-Semantically Wrong Msg
- 2G-Semantically Wrg Msg
- 3G-Invalid Mandatory Info
- 2G-Invalid Mandatory Info
- 3G-MSG type Non Existent
- 2G-MSG type Non Existent
- 3G-MSG type not compatible with protocol state
- 2G-MSG type not compatible with protocol state
- 3G-IE Non Existent
- 2G-IE Non Existent
- 3G-Conditional IE Error
- 2G-Conditional IE Error
- 3G-Message not compatible with protocol state

- 2G-Message not compatible with protocol state
- 3G-Protocol Error
- 2G-Protocol Error
- 3G-Unknown cause
- 2G-Unknown cause

- Inter Service Comb. Routing Area Update Reject Causes:
  - 3G-IMSI Unknown in HLR
  - 2G-IMSI Unknown in HLR
  - 3G-Illegal MS
  - 2G-Illegal MS
  - 3G-Illegal ME
  - 2G-Illegal ME
  - 3G-GPRS service not allowed
  - 2G-GPRS service not allowed
  - 3G-GPRS and Non-GPRS service not allowed
  - 2G-GPRS and Non-GPRS service not allowed
  - 3G-MsId not derived by Nw
  - 2G-MsId not derived by Nw
  - 3G-Implicitly Detached
  - 2G-Implicitly Detached
  - 3G-PLMN not allowed
  - 2G-PLMN not allowed
  - 3G-Location Area not allowed
  - 2G-Location Area not allowed
  - 3G-Roaming not allowed in this Location Area
  - 2G-Roaming not allowed in this Location Area
  - 3G-GPRS service not allowed in this PLMN
  - 2G-GPRS service not allowed in this PLMN
  - 3G-No suitable cells in this Location Area
  - 2G-No suitable cells in this Location Area
  - 3G-MSC not reachable
  - 2G-MSC not reachable
  - 3G-Network Failure
  - 2G-Network Failure
  - 3G-MAC Failure
  - 2G-MAC Failure
  - 3G-SYNC Failure
  - 2G-SYNC Failure

- 3G-Congestion
- 2G-Congestion
- 3G-GSM Auth Unacceptable
- 2G-GSM Auth Unacceptable
- 3G-No PDP contexts activated
- 2G-No PDP contexts activated
- 3G-Retry from new cell
- 2G-Retry from new cell
- 3G-Semantically Wrong Msg
- 2G-Semantically Wrg Msg
- 3G-Invalid Mandatory Info
- 2G-Invalid Mandatory Info
- 3G-MSG type Non Existent
- 2G-MSG type Non Existent
- 3G-MSG type not compatible with protocol state
- 2G-MSG type not compatible with protocol state
- 3G-IE Non Existent
- 2G-IE Non Existent
- 3G-Conditional IE Error
- 2G-Conditional IE Error
- 3G-Message not compatible with protocol state
- 2G-Message not compatible with protocol state
- 3G-Protocol Error
- 2G-Protocol Error
- 3G-Unknown cause
- 2G-Unknown cause

CLI (Exec Mode)

`show gmm-sm statistics [ verbose ]`

Web Element Manager Path

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

show gtpp counters all

The output of this command is now enhanced for Ga interface support to SGSN with the following counters:

- Outstanding M-CDRs
- Possibly Duplicate Outstanding M-CDRs
- Archived M-CDRs
- M-CDRs buffered with AAAPROXY

- M-CDRs buffered with AAAMGR
- Outstanding S-CDRs
- Possibly Duplicate Outstanding S-CDRs
- Archived S-CDRs
- S-CDRs buffered with AAAPROXY
- S-CDRs buffered with AAAMGR
- Outstanding S-SMO-CDRs
- Possibly Duplicate Outstanding S-SMO-CDRs
- Archived S-SMO-CDRs
- S-SMO-CDRs buffered with AAAPROXY
- S-SMO-CDRs buffered with AAAMGR
- Outstanding S-SMT-CDRs
- Possibly Duplicate Outstanding S-SMT-CDRs
- Archived S-SMT-CDRs
- S-SMT-CDRs buffered with AAAPROXY
- S-SMT-CDRs buffered with AAAMGR
- Outstanding GMBH CDRs
- Possibly Duplicate Outstanding GMBH CDRs
- Archived GMBH CDRs
- GMBH CDRs buffered with AAAPROXY
- GMBH CDRs buffered with AAAMGR

CLI (Exec Mode)

```
show gtpp counter all
```

Web Element Manager Path

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

show gtpp storage-server

A new keyword has been added to this command to display statistics and counters for files stored on the SMC hard disk.

CLI (Exec Mode)

```
show gtpp storage-server local file { counters | statistics }
```

Web Element Manager Path

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

show gtpp storage-server statistics

The output of this command is now enhanced for M-CDRs and S-CDRs for SGSN with the following counters:

- Store Requests (M-CDRs)
  - Sent
  - Retried
  - Success
  - Failed
- Store Requests (S-CDRs)
  - Sent
  - Retried
  - Success
  - Failed

CLI (Exec Mode)

`show gtpp cstorage-server statistics`

Web Element Manager Path

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

show iups-service

This command has been modified to limit the display of information to a specific RNC.

CLI (Exec Mode)

`show iups-service { all | name srvc_name }[ rnc { all | mcc mcc_num mnc mnc_num } ]`

Web Element Manager Path

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

show sccp-network

There are new keywords (**`status all`** and **`status dpc`**) to fine tune the displayed information for the SCCP networks.

CLI (Exec Mode)

`show sccp-network { ntwk_index | all } [ status [ all | dpc ] ]`

Web Element Manager Path

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

show session disconnect-reasons verbose

The output of this command is now enhanced for SGSN related disconnect reason with the following counters:

- sgsn-attach-in-reg-state(291)
- sgsn-inbound-srns-in-reg-state(292)
- dt-ggsn-tun-reestablish-failed(293)

CLI (Exec Mode)

show session disconnect-reasons [verbose]

Web Element Manager Path

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

show session subsystem

The output of this command is now enhanced for S-CDRs, M-CDRs, S-SMO-CDRs, and S-SMT-CDRs with following counters:

- Total S-CDRs
- Current S-CDRs
- Total M-CDRs
- Current M-CDRs
- Total S-SMO-CDRs
- Current S-SMO-CDRs
- Total S-SMT-CDRs
- Current S-SMT-CDRs

CLI (Exec Mode)

show session subsystem [**full** | **facility** *facility* [**all** | **instance** *id*]] [**verbose**] [**|** { **grep** *grep_options* | **more** }]

Web Element Manager Path

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

show sgtp-service

The new keyword “sgsn-table” added to this command to show SGSN information.

CLI (Exec Mode)

show sgtp-service { all | ggsn-table | sgsn-table | name *srvc_name* }

Web Element Manager Path

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

show ss7-routing-domain

This command is enhanced to display the SS7 domain related statistics for following protocols with different filter options:

- SSCF: Service Specific Coordination Function (q.2140)
- QSAAL: Signaling ATM Adaption Layer (SAAL)
- MTP3: SS7 Message Transfer Part-3
- M3UA: SS7 MTP3 User Adaptation Layer
- SCTP ASP: Stream Control Transmission Protocol (SCTP) application server process

CLI (Exec Mode)

show ss7-routing-domain *domain_index* **{ sscf | qsaal | mtp3 } { status | statistics } linkset [all | id** *linkset_id***] link [all | id** *link_id* **] {verbose}**

show ss7-routing-domain *domain_index* **m3ua { status | statistics } { all | peer-server [all | id** *peer_id***] {{verbose} | peer-server-process [all | instance** *instance_id***]}} {verbose}**

show ss7-routing-domain *domain_index* **sctp asp [all | instance** *instance_id* **] statistics { gen | end-point }{verbose}**

show ss7-routing-domain *domain_index* **mtp3 { status | statistics } { gen | destination-point-code [all |** *dest_point_code* **] | linkset [all | id** *linkset_id* **] {link [all | id** *link_id* **]}} {verbose}**

Web Element Manager Path

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

show ss7-routing-domain

This command has been enhanced in several ways - 1) with the ‘all’ keyword to display all SS7RD information with one command; 2) with the ‘mtp2’ keyword to access a display of statistics or status information for the MTP2 layer; and 3) to display routing tables.:

- MTP2: SS7 Message Transfer Part-2
- routes tables (with or without adjacent point codes)

CLI (Exec Mode)

show ss7-routing-domain { all | ss7rd_id { m3ua | mtp2 | mtp3 | qsaal | routes [adjacent] | sctp asp { all | instance asp_id } | sscf } }

Web Element Manager Path

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

show subscriber

New filter keyword **nsapi** added to this existing command to show the subscriber information on the basis of network service access point identifier (NSAPI).

CLI (Exec Mode)

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

Web Element Manager Path

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

show subscriber

New filter keywords **`gprs-only and sgsn-only have been`** added to this existing command, used with valid filters, to focus the output to information for 2G or 3G SGSN connections/contexts.

CLI (Exec Mode)

`show subscribers` [gprs-only | sgsn-only] [*`filter_keywords`*] [**`|`** { **`grep`** *`grep_options`* | **`more`**}]

Web Element Manager Path

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

show sgtpu statistics

The output of this command is now enhanced with the following pairs of counters:

- Total Packets Rcvd
  - Iu Release
  - T3-tunnel Timer expiry
- Total Bytes Rcvd
  - Iu Release
  - T3-tunnel Timer expiry

CLI (Exec Mode)

`show sgtpu statistics [ ggsn-address` *`ipv4_address`* | **`iups-service`** *`iups_srvc_name`* | **`rnc-address`** *`ipv4_address`* | **`sgtp-service`** *`sgtp_srvc_name`* | **`gprs-service`** *`gprs_srvc_name`* **`nsei`** *`nse_id`* **`]`**

Web Element Manager Path

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

show llc statistics

A new counter, **Unit data requests Rx Drop** is added to count the number of down link unit data packets (received from SNDCP) dropped by LLC.

CLI (Exec Mode)

`show llc statistics [ verbose ]`

Web Element Manager Path

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

show sndcp statistics verbose

The output of this command is now enhanced with the following PDU Drop Reason counters:

- SN-PDU Drop Reason
  - Invalid SAPI State
  - Invalid PDP Ctx
  - Decode Failure
- Reassembly Drops
  - Discard State
  - Rx First Seg State
  - Rx Subsequent Seg State
  - New First Segment
  - Reassembly Failure
  - Reassembly Timeout
- DCOMP Error
- PCOMP Error
- PDP Ctx Modified
- PDP Ctx Deleted
- Other Reasons

CLI (Exec Mode)

```
show sndcp statistics [ verbose ]
```

Web Element Manager Path

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

show sgtpu statistics

The output of this command is now enhanced with the following pairs of counters:

- Total Packets Rcvd
  - Pkts forward from queue
  - BVC Reset/Block Rcvd
- Total Bytes Rcvd
  - Bytes forward from queue
  - BVC Reset/Block Rcvd

CLI (Exec Mode)

```
show sgtpu statistics [ ggsn-address ipv4_address | iups-service
iups_srvc_name | rnc-address ipv4_address | sgtp-service sgtp_srvc_name |
gprs-service gprs_srvc_name nsei nse_id ]
```

Web Element Manager Path

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

show sgtpu statistics

The output of this command is now enhanced with the following counters to count the packets and bytes that are dropped due to DP session in suspended state:

- Total Packets Rcvd
  - Pkts when dp suspended
- Total Bytes Rcvd
  - Pkts when dp suspended

CLI (Exec Mode)

show sgtpu statistics [ggsn-address *ipv4_address* | **iups-service** *iups_srvc_name* | **rnc-address** *ipv4_address* | **sgtp-service** *sgtp_srvc_name* | **gprs-service** *gprs_srvc_name* **nsei** *nse_id* **]**

Web Element Manager Path

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

show gprs-service all

The output of this command is now enhanced with the “SM-Ignore PCO IE Decode Error” parameter to ignore decoding error due to incorrect PCO IE length in SM messages.

CLI (Exec Mode)

show gprs-service all

Web Element Manager Path

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

show gprs-service all

The output of this command is now enhanced with the following counters:

- SM-Trim Trailing Spaces in APN
- SM-APN Partial match

CLI (Exec Mode)

show gprs-service all

Web Element Manager Path

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

show gmm-sm statistics

The output of this command is now enhanced with the following counters:

- Auth Triplets Reuse Counter
  - 3G-Auth Triplets Reuse
  - 2G-Auth Triplets Reuse

CLI (Exec Mode)

show gmm-sm statistics [verbose]

Web Element Manager Path

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

show gprs-service all

The output of this command is now enhanced with the “SM-APN(R) from First Sub Record” parameter to enable/disable APN from the first subscription record to be used in the requested APN.

CLI (Exec Mode)

```
show gprs-service all
```

Web Element Manager Path

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

SGSN Commands - Modified in Release 8.1

clear sgtpu-statistics

Adds a new keyword set **gprs-service - nsei** to clear statistics for a specific NSEI associated with the specified GPRS service in the current context.

CLI (Exec Mode)

clear sgtpu statistics [ggsn-address *ipv4_address* **| iups-service** *iups_srvc_name* **| rnc-address** *ipv4_address* **| sgtp-service** *sgtp_srvc_name* **| gprs-service** *gprs_srvc_name* **nsei** *nse_id* **]**

Web Element Manager Path

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

show gmm-sm statistics

The output of this command is now enhanced with the following two counters to count the current number of supporting and non-supporting Network Sharing Subscribers in the system:

- Network Sharing Subscribers
  - 3G-Supporting-UE
  - 3G-Non-Supporting-UE

CLI (Exec Mode)

show gmm-sm statistics [gmm-only | sm-only] [gprs-service *srvc_name* **[nsei** *nse_id* **| routing-area mcc** *mc_code* **mnc** *mn_code* **lac** *loc_code* **rac** *ra_code* **]] | [sgsn-service** *srvc_name* **[rnc mcc** *mc_code* **mnc** *mn_code* **rnc-id** *rnc_id* **| routing area mcc** *mc_code* **mnc** *mn_code* **lac** *loc_code* **rac** *ra_code* **]] [verbose] [| { grep** *grep_options* **| more }]**

Web Element Manager Path

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

show gmm-sm statistics verbose

The output of this command is now enhanced with the following two counters:

- 3G-Phase-2-Offload Failures
- 2G-Phase-2-Offload Failures

CLI (Exec Mode)

show gmm-sm statistics [verbose]

Web Element Manager Path

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

show iups-service

This command has been modified to limit the display of information to a specific RNC.

CLI (Exec Mode)

show iups-service { all | name *srvc_name* }[rnc { all | *rnc_id* }]

Web Element Manager Path

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

show sgtpu-statistics

Adds a new keyword set **gprs-service - nsei** to display the statistics for a specific NSEI-based GTPU stats associated with the specified GPRS service in the current context.

CLI (Exec Mode)

show sgtpu statistics [ggsn-address *ipv4_address* **| iups-service** *iups_srvc_name* **| rnc-address** *ipv4_address* **| sgtp-service** *sgtp_srvc_name* | **gprs-service** *gprs_srvc_name* **nsei** *nse_id* **]**

Web Element Manager Path

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

show gmm-sm statistics

The output of this command is now enhanced with the following counters:

- Redirection Indication
  - PLMN not allowed
  - Location area not allowed
  - Roaming not allowed in LA
  - No GPRS services in PLMN
  - CS/PS co-ord required
  - Unknown Reasons

CLI (Exec Mode)

show gmm-sm statistics [gmm-only | sm-only] [gprs-service *srvc_name* **[nsei** *nse_id* **| routing-area mcc** *mc_code* **mnc** *mn_code* **lac** *loc_code* **rac** *ra_code* **]] | [sgsn-service** *srvc_name* **[rnc mcc** *mc_code* **mnc** *mn_code* **rnc-id** *rnc_id* **| routing area mcc** *mc_code* **mnc** *mn_code* **lac** *loc_code* **rac** *ra_code* **]] [verbose] [| { grep** *grep_options* **| more }]**

Web Element Manager Path

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

show gmm-sm statistics

The output of this command is now enhanced with the following counters:

- Detach Request
  - 3G-Nw-Init-Reatch-Req
  - 2G-Nw-Init-Reatch-Req
  - 3G-Nw-Init-Reatch-Not-Req
  - 2G-Nw-Init-Reatch-Not-Req
  - 3G-Nw-Init-IMSI-Detach
  - 2G-Nw-Init-IMSI-Detach
- Retransmission
  - Ret-3G-Nw-Init-Reatch-Req
  - Ret-2G-Nw-Init-Reatch-Req
  - Ret-3G-Nw-Init-Reatch-Not
  - Ret-2G-Nw-Init-Reatch-Not
  - Ret-3G-Nw-Init-IMSI-Detach
  - Ret-2G-Nw-Init-IMSI-Detach

CLI (Exec Mode)

show gmm-sm statistics [gmm-only | sm-only] [gprs-service *srvc_name* **[nsei** *nse_id* **| routing-area mcc** *mc_code* **mnc** *mn_code* **lac** *loc_code* **rac** *ra_code* **]] | [sgsn-service** *srvc_name* **[rnc mcc** *mc_code* **mnc** *mn_code* **rnc-id** *rnc_id* **| routing area mcc** *mc_code* **mnc** *mn_code* **lac** *loc_code* **rac** *ra_code* **]] [verbose] [| { grep** *grep_options* **| more }]**

Web Element Manager Path

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

show gmm-sm statistics verbose

The output of this command is now enhanced with the following counters:

- Retransmission
  - Ret-3G-Nw-Init-Reatch-Req
  - Ret-2G-Nw-Init-Reatch-Req
  - Ret-3G-Nw-Init-Reatch-Not
  - Ret-2G-Nw-Init-Reatch-Not
  - Ret-3G-Nw-Init-IMSI-Detach
  - Ret-2G-Nw-Init-IMSI-Detach

CLI (Exec Mode)

show gmm-sm statistics [verbose]

Web Element Manager Path

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

show subscribers sgsn-only full

The counter ‘Network Sharing Capability’ has been added to the output of this command to indicate if the MS supports network sharing or not.

CLI (Exec Mode)

show subscribers sgsn-only full [| { grep *grep_options* **| more }]**

Web Element Manager Path

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

show sgtpu statistics

The output of this command is now enhanced with the following counters:

- Total Error Ind Sent
  - Sent to GGSN
  - Sent to RNC
- Total Error Ind Rcvd
  - Rcvd from GGSN
  - Rcvd from RNC
  - Rcvd from GGSN through RNC
  - Rcvd from RNC through GGSN

CLI (Exec Mode)

show sgtpu statistics [ggsn-address *ipv4_address* | **iups-service** *iups_srvc_name* | **rnc-address** *ipv4_address* | **sgtp-service** *sgtp_srvc_name* | **gprs-service** *gprs_srvc_name* **nsei** *nse_id* **]**

Web Element Manager Path

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

show gmm-sm statistics verbose

The output of this command is now enhanced with the following counters:

2G APN Selection Failure Statistics:

- SDL-1:
  - All Packet Services Barred
  - PDP Type not Present, PDP Address Present
  - PDP Type not Present, APN Present
  - PDP Type, Address and APN not Present, No Single SubRec
- SDL-2:
  - No SubRec matching PDP Type
  - No SubRec matching PDP Type and APN, No Wildcard APN
  - Multiple SubRecs matching PDP Type and APN, No Dynamic Address
  - Multiple SubRecs matching PDP Type and APN, with Dynamic Address

- SDL-3:
  - APN not Present
  - No Wildcard APN, Multiple SubRecs matching PDP Type
  - Multiple SubRecs with Wildcard APN and same PDP Type
  - PDP Address Present
  - No SubRec matching PDP Address
  - Single SubRec matching PDP Address, No APN Match
  - Multiple SubRecs matching PDP Address, APN not requested
  - Multiple SubRecs matching PDP Address, No APN Match
- SDL-4:
  - APN sent by MS
  - VPLMN User, APN-OI not HPLMN, not VPLMN
  - VPLMN User, APN-OI is VPLMN, VPLMN Addr not allowed
  - VPLMN User, APN-OI is VPLMN, VPLMN AP Barred
  - VPLMN User, APN-OI is HPLMN, HPLMN AP Barred
  - VPLMN User, No APN-OI, VPLMN Addr not allowed, HPLMN AP Barred
  - VPLMN User, No APN-OI, VPLMN AP Barred, HPLMN AP Barred
  - HPLMN user, APN-OI not HPLMN
  - APN from Single Context
  - VPLMN Addr not allowed, HPLMN AP Barred
  - VPLMN AP Barred, HPLMN AP Barred
- SDL-5:
  - VPLMN User, VPLMN Addr not allowed
  - VPLMN User, VPLMN AP Barred
  - No Default APN for PDP Type
  - Internal APN Selection Failures
  - Wildcard APN with Static Address
  - Unknown PDP Type in Subscribed Record

CLI (Exec Mode)

```
show gmm-sm statistics [ verbose ]
```

Web Element Manager Path

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

Obsoleted Commands

The following commands were obsoleted from either Release 8.0 or 8.1.

Common Commands - Obsoleted from Release 8.0

No common commands were obsoleted from Release 8.0.

Common Commands - Obsoleted from Release 8.1

No common commands were obsoleted from Release 8.1.

CF Commands - Obsoleted from Release 8.0

No CF commands were obsoleted from Release 8.0.

CF Commands - Obsoleted from Release 8.1

show content-filtering category policy-id

This command displays Content Filtering category policy definitions. This command is replaced by the **show active-charging content-filtering category policy-id** command.

CLI (Exec Mode)

show content-filtering category policy-id { all | id *cf_policy_id* **} [| { grep** *grep_options* **| more }]**

Web Element Manager Path

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

ECS Commands - Obsoleted from Release 8.0

No ECS commands were obsoleted from Release 8.0.

ECS Commands - Obsoleted from Release 8.1

No ECS commands were obsoleted from Release 8.1.

Firewall Commands - Obsoleted from Release 8.0

clear firewall flows

This command clears the active firewall flows based on different criteria and also clears the disconnect reason information of disconnected flows.

CLI (Exec Mode)

clear firewall flows {active { all | callid *call_id* **| imsi** *num* **| msid** *num* **| username** *name* **} | disconnect-reasons } [-noconfirm]**

Web Element Manager Path

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

clear firewall ruledef

This command clears statistics of the firewall rule definitions (Ruledefs) based on Ruledef name.

CLI (Exec Mode)

clear firewall ruledef statistics [name *ruledef_name* **] [| { grep** *grep_options* **| more }]**

Web Element Manager Path

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

clear firewall statistics

This command clears the statistics of firewall session based on different criteria.

CLI (Exec Mode)

clear firewall statistics [callid *call_id* **| destination** *ip_address* **[port** *dest_port* **] | domain-name** *domain_name* **| protocol { icmp | other | tcp | udp } | source** *ip_address* **[port** *source_port* **] [destination** *ip_address* **[port** *dest_port* **]] | username** *name* **] [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.

show firewall flows

This command displays the active firewall flows based on different criteria and also the reasons for disconnected flows.

CLI (Exec Mode)

show firewall flows { active { all | callid *call_id* **| imsi** *num* **| msid** *num* **| username** *name* **} [verbose] | disconnect-reasons } [| { grep** *grep_options* **| more }]**

Web Element Manager Path

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

show firewall ruledef

This command displays the firewall rule definitions (Ruledefs) based on different criteria with statistical information.

CLI (Exec Mode)

show firewall ruledef {all | name *ruledef_name* **| statistics [name** *ruledef_name* **] } [| { grep** *grep_options* **| more }]**

Web Element Manager Path

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

show firewall statistics

This command displays the statistics of firewall session based on different criteria.

CLI (Exec Mode)

show firewall statistics [callid *call_id* **| destination** *ip_address* **[port** *dest_port* **] | domain-name** *domain_name* **| protocol { icmp | other | tcp | udp } | source** *ip_address* **[port** *source_port* **] [destination** *ip_address* **[port** *dest_port* **]] | username** *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.

update firewall policy

This command updates/changes the firewall access policy for the specified active subscriber session.

CLI (Exec Mode)

update firewall policy { all | callid *call_id* **| context** *context_name* **| imsi** *imsi_num* **| ip-address** *ip_address* **| msid** *msid_num* **| username** *user_name* **} policy-name** *policy_name* **[verbose] [-noconfirm] [| { grep** *grep_options* **| more }]**

Web Element Manager Path

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

Firewall Commands Obsoleted from Release 8.1

No Firewall commands were obsoleted from Release 8.1.

GGSN Commands - Obsoleted from Release 8.0

No GGSN commands were obsoleted from Release 8.0.

GGSN Commands - Obsoleted from Release 8.1

No GGSN commands were obsoleted from Release 8.1.

HA Commands - Obsoleted from Release 8.0

No HA commands were obsoleted from Release 8.0.

HA Commands - Obsoleted from Release 8.1

No HA commands were obsoleted from Release 8.1.

PDSN Commands - Obsoleted from Release 8.0

No PDSN commands were obsoleted from Release 8.0.

PDSN Commands - Obsoleted from Release 8.1

No PDSN commands were obsoleted from Release 8.1.

SGSN Commands - Obsoleted from Release 8.0

No SGSN commands were obsoleted from Release 8.0.

SGSN Commands - Obsoleted from Release 8.1

No SGSN commands were obsoleted from Release 8.1.

GTPP Storage Server Changes

There were no GSS changes in Release 8.0 or 8.1.

Web Element Manager Changes

There were no Web Element manager changes in Release 8.0 or 8.1.

CHAPTER 6
SECURITY MANAGEMENT

This section contains additions and changes made to the security features available in Release 8.0 unless specifically designated as being in Release 8.1.

Security Enhancements

New Commands

The following new commands were added for Release 8.0 and 8.1.

cli login-failure-delay

This is the time to wait in seconds between a login failure returned and another login attempt.

CLI (Global Configuration Mode)

`[ no | default ] CLI login-failure-delay` *`time`*

Web Element Manager Path

Click Configuration | Context configuration

Modified Commands

There were no modified commands for Release 8.0 and 8.1.

Obsoleted Commands

There were no obsoleted commands for Release 8.0 and 8.1.