



## **Cisco ASR 5000 Series Gateway GPRS Support Node Administration Guide**

**Version 12.2**

**Last updated April 30, 2012**

### **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-25637-02

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.

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](http://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.

Cisco ASR 5000 Series Gateway GPRS Support Node Administration Guide

© 2012 Cisco Systems, Inc. and/or its affiliated entities. All rights reserved.

# CONTENTS

---

<b>About this Guide .....</b>	<b>xvii</b>
Conventions Used .....	xviii
Contacting Customer Support .....	xx
Additional Information .....	xxi
<b>GGSN Support in GPRS/UMTS Wireless Data Services .....</b>	<b>23</b>
Product Description .....	24
Product Specification .....	25
Licenses .....	25
Platform Requirements .....	25
Operating System Requirements .....	25
Network Deployment and Interfaces .....	26
GGSN in the GPRS/UMTS Data Network .....	26
Supported Interfaces .....	28
Features and Functionality - Base Software .....	31
16,000 SGSN Support .....	32
AAA Server Groups .....	32
Access Control List Support .....	32
ANSI T1.276 Compliance .....	33
APN Support .....	33
Bulk Statistics Support .....	34
Direct Tunnel Support .....	35
DHCP Support .....	36
DSCP Marking .....	37
Framed-Route Attribute Support .....	37
Generic Corporate APN .....	37
GnGp Handoff Support .....	37
GTPP Support .....	38
Host Route Advertisement .....	39
IP Policy Forwarding .....	40
IP Header Compression - Van Jacobson .....	40
IPv6 Support .....	41
Management System Overview .....	42
MPLS Forwarding with LDP .....	43
Overlapping IP Address Pool Support .....	44
PDP Context Support .....	44
Per APN Configuration to Swap out Gn to Gi APN in CDRs .....	45
Port Insensitive Rule for Enhanced Charging Service .....	45
Quality of Service Support .....	46
RADIUS Support .....	46
RADIUS VLAN Support .....	47
Routing Protocol Support .....	48
Subscriber Session Trace Support .....	49
Support of Charging Characteristics Provided by AAA Server .....	51
Support of all GGSN generated causes for partial G-CDR closure .....	51
Threshold Crossing Alerts (TCA) Support .....	51

Features and Functionality - Optional Enhanced Feature Software.....	53
Common Gateway Access Support .....	53
Dynamic RADIUS Extensions (Change of Authorization) .....	54
GRE Protocol Interface Support.....	54
Gx Interface Support .....	56
Inter-Chassis Session Recovery .....	57
IP Security (IPSec) .....	58
L2TP LAC Support .....	60
L2TP LNS Support .....	61
Lawful Intercept .....	61
Mobile IP Home and Foreign Agents .....	62
Mobile IP NAT Traversal .....	63
Multimedia Broadcast Multicast Services Support .....	63
Overcharging Protection on Loss of Coverage .....	63
Proxy Mobile IP .....	64
Session Persistence .....	64
Session Recovery Support .....	65
Traffic Policing and Rate Limiting.....	66
Web Element Management System.....	67
How GGSN Works .....	69
PDP Context Processing.....	69
Dynamic IP Address Assignment .....	70
Subscriber Session Call Flows.....	71
Transparent Session IP Call Flow.....	71
Non-Transparent IP Session Call Flow.....	73
Network-Initiated Session Call Flow .....	76
PPP Direct Access Call Flow .....	77
Virtual Dialup Access Call Flow .....	79
Corporate IP VPN Connectivity Call Flow .....	81
Mobile IP Call Flow .....	83
Proxy Mobile IP Call Flows .....	86
IPv6 Stateless Address Auto Configuration Flows .....	89
Supported Standards.....	91
3GPP References.....	91
IETF References .....	92
Object Management Group (OMG) Standards .....	95
<b>Understanding the Service Operation .....</b>	<b>97</b>
Terminology .....	98
Contexts .....	98
Logical Interfaces .....	99
Bindings.....	100
Services.....	101
How the System Selects Contexts .....	103
Context Selection for Subscriber Sessions .....	103
<b>GGSN Configuration Example .....</b>	<b>105</b>
Information Required .....	107
Source Context Configuration .....	107
Destination Context Configuration.....	110
How This Configuration Works .....	115
Transparent IP PDP Context Processing .....	115
Non-transparent IP PDP Context Processing .....	117
PPP PDP Context Processing.....	118
Network-requested PDP Context Processing .....	120



<b>Mobile IP Configuration Examples .....</b>	<b>123</b>
Example 1: Mobile IP Support Using the System as a GGSN/FA .....	124
Information Required .....	125
Source Context Configuration .....	125
AAA Context Configuration .....	128
Mobile IP Destination Context Configuration .....	130
Optional Destination Context Configuration .....	132
How This Configuration Works .....	133
Example 2: Mobile IP Support Using the System as an HA .....	136
Information Required .....	137
Source Context Configuration .....	137
Destination Context Configuration .....	140
How This Configuration Works .....	141
Example 3: HA Using a Single Source Context and Multiple Outsourced Destination Contexts .....	143
Information Required .....	145
Source Context Configuration .....	145
Destination Context Configuration .....	148
System-Level AAA Configuration .....	150
How This Configuration Works .....	150
<b>GGSN and Mobile IP Service in a Single System Configuration Example</b>	<b>153</b>
Using the System as Both a GGSN/FA and an HA .....	154
Information Required .....	155
Source Context Configuration .....	155
Destination Context Configuration .....	158
Mobile IP Destination Context Configuration .....	162
How This Configuration Works .....	166
<b>GGSN Service Configuration Procedures .....</b>	<b>169</b>
GGSN Service Configuration .....	170
GGSN Service Creation and Binding .....	170
Accounting Context and Charging Characteristics Configuration .....	171
SGSN and PLMN Policy Configuration .....	171
Network-requested PDP Context Support Configuration .....	172
GGSN Configuration Verification .....	172
GTPP Accounting Support Configuration .....	176
GTPP Group Creation .....	177
GTPP Group Configuration .....	177
GTPP Group Configuration Verification .....	178
APN Configuration .....	179
APN Creation and Configuration .....	179
Authentication, Accounting, and GTPP Group Configuration in APN .....	180
Authentication and Accounting Configuration in APN .....	180
GTPP Group Association to APN .....	181
IP Address Allocation Method Configuration in APN .....	181
Charging Characteristics Parameter Configuration in APN .....	182
Virtual APN Configuration .....	182
Other Optional Parameter Configuration in APN .....	183
APN Configuration Verification .....	183
DHCP Service Configuration .....	188
DHCP Service Creation .....	188
DHCP Server Parameter Configuration .....	189
DHCP Service Configuration Verification .....	189
IP Address Pool Configuration on the System .....	191

IPv4 Pool Creation.....	192
IPv6 Pool Creation.....	192
IP Pool Configuration Verification.....	192
Gn-Gp Handoff Support Configuration .....	194
GTP-U Service Configuration.....	194
Modifying GGSN Configuration for Gn-Gp Handoff .....	195
APN Configuration for Gn-Gp Handoff .....	195
Gn-Gp Configuration Verification .....	196
FA Services Configuration .....	197
FA Service Creation .....	197
IP Interface and UDP Port Binding for Pi Interface .....	198
Security Parameter Index (SPI) Configuration .....	198
FA Agent Advertisement Parameter Configuration .....	199
Subscriber Registration, Authentication and Timeout Parameter Configuration.....	200
Revocation Message Configuration .....	201
FA Service Configuration Verification.....	201
Common Gateway Access Support Configuration .....	203
Diameter Endpoint Configuration .....	203
AAA Group Configuration.....	204
Authorization over S6b Configuration.....	204
DNS Client Configuration .....	204
Duplicate Call Accept Configuration.....	205
Common Gateway Access Support Configuration Verification .....	205
Rf Interface Configuration for Offline Charging .....	207
Accounting Policy Configuration.....	207
Diameter End-Point Configuration.....	207
AAA Group Configuration .....	208
APN Configuration for Rf Interface.....	208
Rf Interface Configuration Verification.....	208
<b>Monitoring the Service .....</b>	<b>211</b>
Monitoring System Status and Performance .....	212
Clearing Statistics and Counters .....	216
<b>Configuring Subscriber Session Trace Support.....</b>	<b>217</b>
Introduction .....	218
Supported Functions .....	219
Supported Standards.....	221
Supported Networks and Platforms .....	222
Licenses.....	223
Subscriber Session Trace Functional Description.....	224
Operation.....	224
Trace Session .....	224
Trace Recording Session.....	224
Network Element (NE).....	224
Activation .....	224
Management Activation.....	225
Signaling Activation.....	225
Start Trigger.....	225
Deactivation .....	225
Stop Trigger .....	225
Data Collection and Reporting .....	225
Trace Depth .....	225
Trace Scope.....	226
Network Element Details .....	226

GGSN.....	226
Subscriber Session Trace Configuration.....	227
Enabling Subscriber Session Trace on UMTS Network Element.....	227
Trace File Collection Configuration.....	228
Trace Collection Entity Configuration.....	228
Verifying Your Configuration.....	229
<b>Troubleshooting the Service .....</b>	<b>231</b>
Test Commands.....	232
Using the PPP Echo-Test Command.....	232
Using the GTPC Test Echo Command.....	232
Using the GTPU Test Echo Command.....	233
Using the GTPv0 Test Echo Command.....	234
Using the DHCP Test Command.....	235
Testing GTPP Accounting with a CGF.....	235
Testing GTPP Connectivity with a GSS.....	236
<b>Mobile-IP and Proxy-MIP Timer Considerations .....</b>	<b>237</b>
Call Flow Summary.....	238
Dealing with the.....	240
Controlling the Mobile IP Lifetime on a Per-Domain Basis.....	241
<b>Engineering Rules .....</b>	<b>245</b>
APN Engineering Rules.....	246
DHCP Service Engineering Rules.....	247
GGSN Engineering Rules.....	248
GRE Tunnel Interface and VRF Engineering Rules.....	249
GTP Engineering Rules.....	250
Interface and Port Engineering Rules.....	251
Pi Interface Rules.....	251
FA to HA Rules.....	251
HA to FA.....	251
GRE Tunnel Interface Rule.....	252
Lawful Intercept Engineering Rules.....	253
MBMS Bearer Service Engineering Rules.....	254
Service Engineering Rules.....	255
Subscriber Engineering Rules.....	256
<b>CoA, RADIUS DM, and Session Redirection (Hotlining) .....</b>	<b>257</b>
RADIUS Change of Authorization and Disconnect Message.....	258
CoA Overview.....	258
DM Overview.....	258
License Requirements.....	258
Enabling CoA and DM.....	258
Enabling CoA and DM.....	259
CoA and DM Attributes.....	259
CoA and DM Error-Cause Attribute.....	260
Viewing CoA and DM Statistics.....	261
Session Redirection (Hotlining).....	264
Overview.....	264
License Requirements.....	264
Operation.....	264
ACL Rule.....	264
Redirecting Subscriber Sessions.....	264
Session Limits On Redirection.....	265
Stopping Redirection.....	265

Handling IP Fragments .....	265
Recovery .....	265
AAA Accounting .....	265
Viewing the Redirected Session Entries for a Subscriber .....	265
<b>GRE Protocol Interface .....</b>	<b>271</b>
Introduction .....	272
Supported Standards .....	274
Supported Networks and Platforms .....	275
Licenses .....	276
Services and Application on GRE Interface .....	277
How GRE Interface Support Works .....	278
Ingress Packet Processing on GRE Interface .....	278
Egress Packet Processing on GRE Interface .....	280
GRE Interface Configuration .....	281
Virtual Routing And Forwarding (VRF) Configuration .....	281
GRE Tunnel Interface Configuration .....	282
Enabling OSPF for VRF .....	283
Associating IP Pool and AAA Group with VRF .....	283
Associating APN with VRF .....	284
Static Route Configuration .....	284
Verifying Your Configuration .....	285
<b>Gx Interface Support .....</b>	<b>287</b>
Rel. 6 Gx Interface .....	288
Introduction .....	288
Supported Networks and Platforms .....	288
License Requirements .....	288
Supported Standards .....	289
How it Works .....	289
Configuring Rel. 6 Gx Interface .....	291
Configuring IMS Authorization Service at Context Level .....	292
Verifying IMS Authorization Service Configuration .....	293
Applying IMS Authorization Service to an APN .....	293
Verifying Subscriber Configuration .....	294
Rel. 7 Gx Interface .....	295
Introduction .....	295
Supported Networks and Platforms .....	297
License Requirements .....	297
Supported Standards .....	297
Terminology and Definitions .....	298
Policy Control .....	298
Charging Control .....	301
Policy and Charging Control (PCC) Rules .....	302
PCC Procedures over Gx Reference Point .....	303
Volume Reporting Over Gx .....	305
How Rel. 7 Gx Works .....	308
Configuring Rel. 7 Gx Interface .....	311
Configuring IMS Authorization Service at Context Level .....	311
Applying IMS Authorization Service to an APN .....	313
Configuring Volume Reporting over Gx .....	314
Gathering Statistics .....	315
Rel. 8 Gx Interface .....	317
HA/PDSN Rel. 8 Gx Interface Support .....	317
Introduction .....	317

Terminology and Definitions .....	319
How it Works .....	325
Configuring HA/PDSN Rel. 8 Gx Interface Support.....	327
Gathering Statistics .....	330
P-GW Rel. 8 Gx Interface Support.....	331
Introduction .....	331
Terminology and Definitions .....	331
Rel. 9 Gx Interface.....	336
P-GW Rel. 9 Gx Interface Support.....	336
Introduction .....	336
Terminology and Definitions .....	336
<b>Gy Interface Support .....</b>	<b>341</b>
Introduction .....	342
License Requirements.....	344
Supported Standards .....	344
Features and Terminology.....	345
Charging Scenarios.....	345
Session Charging with Reservation.....	345
Basic Operations.....	345
Re-authorization.....	346
Threshold based Re-authorization Triggers .....	346
Termination Action .....	346
Diameter Base Protocol .....	346
Diameter Credit Control Application.....	347
Quota Behavior .....	348
Supported AVPs .....	360
Unsupported AVPs .....	364
Configuring Gy Interface Support.....	370
Configuring GGSN / P-GW / IPSG Gy Interface Support .....	370
Configuring HA / PDSN Gy Interface Support .....	371
Gathering Statistics .....	373
<b>ICAP Interface Support.....</b>	<b>375</b>
ICAP Interface Support Overview .....	376
Failure Action on Retransmitted Packets .....	377
Supported Networks and Platforms .....	378
License Requirements.....	378
Configuring ICAP Interface Support .....	379
Creating ICAP Server Group and Address Binding .....	379
Configuring ICAP Server and Other Parameters .....	380
Configuring ECS Rulebase for ICAP Server Group.....	380
Configuring Charging Action for ICAP Server Group.....	381
Verifying the ICAP Server Group Configuration.....	381
<b>IP Pool Sharing Protocol.....</b>	<b>383</b>
Overview.....	384
Primary HA Functionality.....	384
Secondary HA Functionality .....	384
Requirements, Limitations, & Behavior .....	385
How IPSP Works .....	386
IPSP Operation for New Sessions .....	386
IPSP Operation for Session Handoffs.....	388
Configuring IPSP Before the Software Upgrade .....	390
Configuring the AAA Server for IPSP.....	390

Enabling IPSP on the Secondary HA .....	391
Enabling IPSP on the Primary HA .....	391
Verifying the IPSP Configuration .....	392
Configuring IPSP After the Software Upgrade .....	393
Disabling IPSP .....	394
<b>IP Header Compression .....</b>	<b>395</b>
Overview .....	396
Configuring VJ Header Compression for PPP .....	397
Enabling VJ Header Compression .....	397
Verifying the VJ Header Compression Configuration .....	397
Configuring RoHC Header Compression for PPP .....	399
Enabling RoHC Header Compression for PPP .....	399
Verifying the Header Compression Configuration .....	400
Configuring Both RoHC and VJ Header Compression .....	401
Enabling RoHC and VJ Header Compression for PPP .....	401
Verifying the Header Compression Configuration .....	402
Configuring RoHC for Use with SO67 in PDSN or HSGW Service .....	403
Enabling RoHC Header Compression with PDSN .....	403
Enabling RoHC Header Compression with HSGW .....	404
Verifying the Header Compression Configuration .....	404
Using an RoHC Profile for Subscriber Sessions .....	405
Creating RoHC Profile for Subscriber using Compression Mode .....	405
Creating RoHC Profile for Subscriber using Decompression Mode .....	406
Applying RoHC Profile to a Subscriber .....	407
Verifying the Header Compression Configuration .....	407
Disabling VJ Header Compression Over PPP .....	408
Disabling VJ Header Compression .....	408
Verifying the VJ Header Compression Configuration .....	408
Disabling RoHC Header Compression Over SO67 .....	410
Disabling RoHC Header Compression .....	410
Verifying the Header Compression Configuration .....	410
Checking IP Header Compression Statistics .....	412
RADIUS Attributes for IP Header Compression .....	413
<b>IP Security .....</b>	<b>415</b>
Overview .....	417
Applicable Products and Relevant Sections .....	418
IPSec Terminology .....	421
Crypto Access Control List (ACL) .....	421
Transform Set .....	421
ISAKMP Policy .....	421
Crypto Map .....	421
Manual Crypto Maps .....	422
ISAKMP Crypto Maps .....	422
Dynamic Crypto Maps .....	422
Implementing IPSec for PDN Access Applications .....	423
How the IPSec-based PDN Access Configuration Works .....	423
Configuring IPSec Support for PDN Access .....	424
Implementing IPSec for Mobile IP Applications .....	426
How the IPSec-based Mobile IP Configuration Works .....	426
Configuring IPSec Support for Mobile IP .....	429
Implementing IPSec for L2TP Applications .....	431
How IPSec is Used for Attribute-based L2TP Configurations .....	431
Configuring Support for L2TP Attribute-based Tunneling with IPSec .....	433

How IPsec is Used for PDSN Compulsory L2TP Configurations .....	434
Configuring Support for L2TP PDSN Compulsory Tunneling with IPsec .....	435
How IPsec is Used for L2TP Configurations on the GGSN .....	436
Configuring GGSN Support for L2TP Tunneling with IPsec .....	437
Transform Set Configuration .....	438
Configuring Transform Set .....	438
Verifying the Crypto Transform Set Configuration .....	438
ISAKMP Policy Configuration .....	440
Configuring ISAKMP Policy .....	440
Verifying the ISAKMP Policy Configuration .....	441
ISAKMP Crypto Map Configuration .....	442
Configuring ISAKMP Crypto Maps .....	442
Verifying the ISAKMP Crypto Map Configuration .....	443
Dynamic Crypto Map Configuration .....	445
Configuring Dynamic Crypto Maps .....	445
Verifying the Dynamic Crypto Map Configuration .....	445
Manual Crypto Map Configuration .....	447
Configuring Manual Crypto Maps .....	447
Verifying the Manual Crypto Map Configuration .....	448
Crypto Map and Interface Association .....	450
Applying Crypto Map to an Interface .....	450
Verifying the Interface Configuration with Crypto Map .....	450
FA Services Configuration to Support IPsec .....	452
Modifying FA service to Support IPsec .....	452
Verifying the FA Service Configuration with IPsec .....	453
HA Service Configuration to Support IPsec .....	454
Modifying HA service to Support IPsec .....	454
Verifying the HA Service Configuration with IPsec .....	455
RADIUS Attributes for IPsec-based Mobile IP Applications .....	456
LAC Service Configuration to Support IPsec .....	457
Modifying LAC service to Support IPsec .....	457
Verifying the LAC Service Configuration with IPsec .....	458
Subscriber Attributes for L2TP Application IPsec Support .....	459
PDSN Service Configuration for L2TP Support .....	460
Modifying PDSN service to Support Attribute-based L2TP Tunneling .....	460
Modifying PDSN service to Support Compulsory L2TP Tunneling .....	461
Verifying the PDSN Service Configuration for L2TP .....	461
Redundant IPsec Tunnel Fail-Over .....	462
Supported Standards .....	462
Redundant IPsec Tunnel Fail-over Configuration .....	463
Configuring Crypto Group .....	463
Modify ISAKMP Crypto Map Configuration to Match Crypto Group .....	464
Verifying the Crypto Group Configuration .....	464
Dead Peer Detection (DPD) Configuration .....	466
Configuring Crypto Group .....	466
Verifying the DPD Configuration .....	467
APN Template Configuration to Support L2TP .....	468
Modifying APN Template to Support L2TP .....	468
Verifying the APN Configuration for L2TP .....	469
IPsec for LTE/SAE Networks .....	470
Encryption Algorithms .....	470
HMAC Functions .....	470
Diffie-Hellman Groups .....	470
Dynamic Node-to-Node IPsec Tunnels .....	471

ACL-based Node-to-Node IPSec Tunnels .....	471
Traffic Selectors.....	471
Authentication Methods.....	472
X.509 Certificate-based Peer Authentication .....	472
Certificate Revocation Lists .....	474
Child SA Rekey Support.....	474
IKEv2 Keep-Alive Messages (Dead Peer Detection) .....	474
E-UTRAN/EPC Logical Network Interfaces Supporting IPSec Tunnels .....	475
IPSec Tunnel Termination.....	476
<b>L2TP Access Concentrator .....</b>	<b>477</b>
Applicable Products and Relevant Sections.....	478
Supported LAC Service Configurations for PDSN Simple IP .....	479
Attribute-based Tunneling .....	479
How The Attribute-based L2TP Configuration Works.....	480
Configuring Attribute-based L2TP Support for PDSN Simple IP .....	480
PDSN Service-based Compulsory Tunneling .....	481
How PDSN Service-based Compulsory Tunneling Works .....	481
Configuring L2TP Compulsory Tunneling Support for PDSN Simple IP .....	482
Supported LAC Service Configurations for the GGSN and P-GW .....	484
Transparent IP PDP Context Processing with L2TP Support .....	485
Non-transparent IP PDP Context Processing with L2TP Support .....	486
PPP PDP Context Processing with L2TP Support.....	487
Configuring the GGSN or P-GW to Support L2TP .....	488
Supported LAC Service Configuration for Mobile IP .....	489
How The Attribute-based L2TP Configuration for MIP Works.....	489
Configuring Attribute-based L2TP Support for HA Mobile IP .....	490
Configuring Subscriber Profiles for L2TP Support .....	492
RADIUS and Subscriber Profile Attributes Used.....	492
RADIUS Tagging Support.....	493
Configuring Local Subscriber Profiles for L2TP Support.....	493
Configuring Local Subscriber .....	494
Verifying the L2TP Configuration .....	494
Tunneling All Subscribers in a Specific Context Without Using RADIUS Attributes.....	495
Configuring LAC Services.....	496
Configuring LAC Service .....	496
Configuring LNS Peer.....	497
Verifying the LAC Service Configuration .....	497
Modifying PDSN Services for L2TP Support.....	499
Modifying PDSN Service .....	499
Verifying the PDSN Service for L2TP Support.....	500
Modifying APN Templates to Support L2TP .....	501
Assigning LNS Peer Address in APN Template.....	501
Configuring Outbound Authentication .....	502
Verifying the APN Configuration.....	502
<b>L2TP Network Server.....</b>	<b>503</b>
LNS Service Operation .....	504
Information Required.....	505
Source Context Configuration .....	505
Destination Context Configuration .....	507
How This Configuration Works.....	508
Configuring the System to Support LNS Functionality .....	511
Creating and Binding LNS Service.....	511
Configuring Authentication Parameters for LNS Service .....	512



Configuring Tunnel and Session Parameters for LNS Service .....	512
Configuring Peer LAC servers for LNS Service .....	513
Configuring Domain Alias for AAA Subscribers .....	513
Verifying the LNS Service Configuration .....	513
<b>Mobile IP Registration Revocation .....</b>	<b>515</b>
Overview .....	516
Configuring Registration Revocation .....	518
Configuring FA Services .....	518
Configuring HA Services .....	518
<b>Multimedia Broadcast and Multicast Service .....</b>	<b>521</b>
Introduction .....	522
Supported Standards .....	524
Supported Networks and Platforms .....	525
Services and Application in MBMS .....	526
MBMS References and Entities .....	526
Gmb Reference .....	526
MBMS UE Context .....	526
MBMS Bearer Context .....	527
Broadcast Multicast Service Center (BM-SC) .....	527
How MBMS Works .....	528
MBMS Broadcast Mode .....	528
MBMS Broadcast Mode Procedure .....	528
MBMS Multicast Mode .....	529
MBMS Multicast Mode Procedure .....	530
MBMS Configuration .....	531
BMSC Profile Configuration .....	531
MBMS GTPP Configuration .....	532
MBMS APN Configuration .....	532
MBMS Provisioning .....	532
Save the Configuration .....	534
Managing Your Configuration .....	535
Gathering MBMS Statistics .....	537
<b>Multi-Protocol Label Switching (MPLS) Support .....</b>	<b>539</b>
Overview .....	540
Chassis as MPLS-CE Connecting to PE .....	540
Chassis as MPLS-CE Connected to ASBR .....	541
Engineering Rules .....	542
Supported Standards .....	543
Supported Networks and Platforms .....	544
Licenses .....	545
Benefits .....	546
Configuring BGP/MPLS VPN with Static Labels .....	547
Create VRF with Route-distinguisher and Route-target .....	547
Set Neighbors and Enable VPNv4 Route Exchange .....	548
Configure Address Family and Redistributed Connected Routes .....	548
Configure IP Pools with MPLS Labels .....	549
Bind DHCP Service for Corporate Servers .....	549
Bind AAA Group for Corporate Servers .....	549
Configuring BGP/MPLS VPN with Dynamic Labels .....	551
Create VRF with Route-distinguisher and Route-target .....	551
Set Neighbors and Enable VPNv4 Route Exchange .....	552
Configure Address Family and Redistributed Connected Routes .....	553

Configure IP Pools with MPLS Labels.....	553
Bind DHCP Service for Corporate Servers .....	553
Bind AAA Group for Corporate Servers .....	554
DSCP and EXP Bit Mapping .....	554
<b>Rejection/Redirection of HA Sessions on Network Failures .....</b>	<b>555</b>
Overview .....	556
Configuring HA Session Redirection .....	557
RADIUS Attributes .....	561
<b>Policy Forwarding.....</b>	<b>563</b>
Overview .....	564
IP Pool-based Next Hop Forwarding .....	565
Configuring IP Pool-based Next Hop Forwarding .....	565
Subscriber-based Next Hop Forwarding .....	566
Configuring Subscriber-based Next Hop Forwarding.....	566
ACL-based Policy Forwarding .....	567
Configuring ACL-based Policy Forwarding .....	567
Applying the ACL to an IP Access Group .....	567
Applying the ACL to a Destination Context.....	567
Applying the ACL to an Interface in a Destination Context.....	568
<b>Proxy-Mobile IP .....</b>	<b>569</b>
Overview .....	570
Proxy Mobile IP in 3GPP2 Service.....	571
Proxy Mobile IP in 3GPP Service.....	571
Proxy Mobile IP in WiMAX Service .....	572
How Proxy Mobile IP Works in 3GPP2 Network .....	573
Scenario 1: AAA server and PDSN/FA Allocate IP Address.....	573
Scenario 2: HA Allocates IP Address .....	575
How Proxy Mobile IP Works in 3GPP Network .....	578
How Proxy Mobile IP Works in WiMAX Network.....	582
Scenario 1: AAA server and ASN GW/FA Allocate IP Address .....	582
Scenario 2: HA Allocates IP Address .....	584
How Proxy Mobile IP Works in a WiFi Network with Multiple Authentication .....	587
Configuring Proxy Mobile-IP Support .....	592
Configuring FA Services.....	592
Verify the FA Service Configuration .....	593
Configuring Proxy MIP HA Failover.....	593
Configuring HA Services .....	594
Configuring Subscriber Profile RADIUS Attributes.....	595
RADIUS Attributes Required for Proxy Mobile IP .....	595
Configuring Local Subscriber Profiles for Proxy-MIP on a PDSN.....	596
Configuring Local Subscriber Profiles for Proxy-MIP on a PDIF .....	597
Configuring Default Subscriber Parameters in Home Agent Context.....	597
Configuring APN Parameters.....	597
<b>QoS Management .....</b>	<b>601</b>
Introduction .....	602
Dynamic QoS Renegotiation .....	603
How Dynamic QoS Renegotiation Works.....	603
Initial QoS.....	603
Service Detection .....	603
Classification of Application Traffic .....	604
QoS Renegotiation for a Subscriber QoS Profile.....	604
Network Controlled QoS (NCQoS) .....	606

How Network Controlled QoS (NCQoS) Works .....	606
Configuring Dynamic QoS Renegotiation.....	608
Configuring ACL for Dynamic QoS Renegotiation .....	608
Configuring Charging Action for Dynamic QoS Renegotiation .....	609
Configuring Rulebase for Dynamic QoS Renegotiation.....	609
Configuring APNs for Dynamic QoS Renegotiation.....	609
Configuring Network Controlled QoS (NCQoS) .....	611
Configuring Packet Filter for NCQoS .....	611
Configuring Charging Action for NCQoS.....	611
Configuring APN for NCQoS.....	612
Monitoring Dynamic QoS Renegotiation Operation .....	613
Event IDs Pertaining to Dynamic QoS Renegotiation.....	613
RADIUS Attributes.....	614
<b>Remote Address-based RADIUS Accounting .....</b>	<b>615</b>
Overview.....	616
License Requirements.....	616
Configuring Remote Address-based Accounting .....	617
Verifying the Remote Address Lists.....	617
Subscriber Attribute Configuration .....	618
Supported RADIUS Attributes.....	618
Configuring Local Subscriber Profiles.....	618
<b>Subscriber Overcharging Protection .....</b>	<b>621</b>
Feature Overview .....	622
Overcharging Protection - GGSN Configuration .....	624
GTP-C Private Extension Configuration.....	624
Verifying Your GGSN Configuration.....	625
Overcharging Protection - SGSN Configuration.....	626
Private Extension IE Configuration .....	626
RANAP Cause Trigger Configuration.....	627
Verifying the Feature Configuration .....	627
<b>Traffic Policing and Shaping .....</b>	<b>629</b>
Overview.....	630
Traffic Policing.....	630
Traffic Shaping .....	630
Traffic Policing Configuration.....	631
Configuring Subscribers for Traffic Policing.....	631
Configuring APN for Traffic Policing in 3GPP Networks .....	632
Traffic Shaping Configuration.....	634
Configuring Subscribers for Traffic Shaping .....	634
Configuring APN for Traffic Shaping in 3GPP Networks .....	635
RADIUS Attributes.....	638
Traffic Policing for CDMA Subscribers.....	638
Traffic Policing for UMTS Subscribers .....	639



# About this Guide

---





This document pertains to the features and functionality that run on and/or that are related to the Cisco® ASR 5x00 Chassis.

This preface includes the following sections:

- [Conventions Used](#)
- [Contacting Customer Support](#)
- [Additional Information](#)

# 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.
	Electrostatic Discharge (ESD)	Warns you to take proper grounding precautions before handling ESD sensitive components or devices.

Typeface Conventions	Description
Text represented as a <i>screen display</i>	This typeface represents text that appears on your terminal screen, for example: <i>Login:</i>
Text represented as <b>commands</b>	This typeface represents commands that you enter at the CLI, for example: <b>show ip access-list</b> This document always gives the full form of a command in lowercase letters. Commands are <u>not</u> case sensitive.
Text represented as a <b>command variable</b>	This typeface represents a variable that is part of a command, for example: <b>show card slot_number</b> <i>slot_number</i> 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 <b>File</b> menu, then click <b>New</b> .

Command Syntax Conventions	Description
{ <b>keyword</b> or <i>variable</i> }	Required keywords and variables are surrounded by braces. They must be entered as part of the command syntax.
[ <b>keyword</b> or <i>variable</i> ]	Optional keywords or variables that may or may not be used are surrounded by brackets.

Command Syntax Conventions	Description
	<p>Some commands support alternative variables. These “options” are documented within braces or brackets by separating each variable with a vertical bar.</p> <p>These variables can be used in conjunction with required or optional keywords or variables. For example:</p> <pre>{ <b>nonce</b>   <b>timestamp</b> }</pre> <p>OR</p> <pre>[ <b>count</b> <i>number_of_packets</i>   <b>size</b> <i>number_of_bytes</i> ]</pre>

## Contacting Customer Support

Go to <http://www.cisco.com/cisco/web/support/> to submit a service request. A valid Cisco account (username and password) is required to access this site. Please contact your Cisco account representative for additional information.



## Additional Information

Refer to the following guides for supplemental information about the system:

- *Command Line Interface Reference*
- *Statistics and Counters Reference*
- *Thresholding Configuration Guide*
- *SNMP MIB Reference*
- *Cisco Web Element Manager Installation and Administration Guide*
- Product-specific and feature-specific administration guides
- *Release Notes* that accompany updates and upgrades to StarOS



# Chapter 1

## GGSN Support in GPRS/UMTS Wireless Data Services

---

The Cisco systems provides wireless carriers with a flexible solution that functions as a Gateway GPRS Support Node (GGSN) in General Packet Radio Service (GPRS) or Universal Mobile Telecommunications System (UMTS) wireless data networks.

This overview provides general information about the GGSN including:

- [Product Description](#)
- [Product Specification](#)
- [Network Deployment and Interfaces](#)
- [Features and Functionality - Base Software](#)
- [Features and Functionality - Optional Enhanced Feature Software](#)
- [How GGSN Works](#)
- [Supported Standards](#)

## Product Description

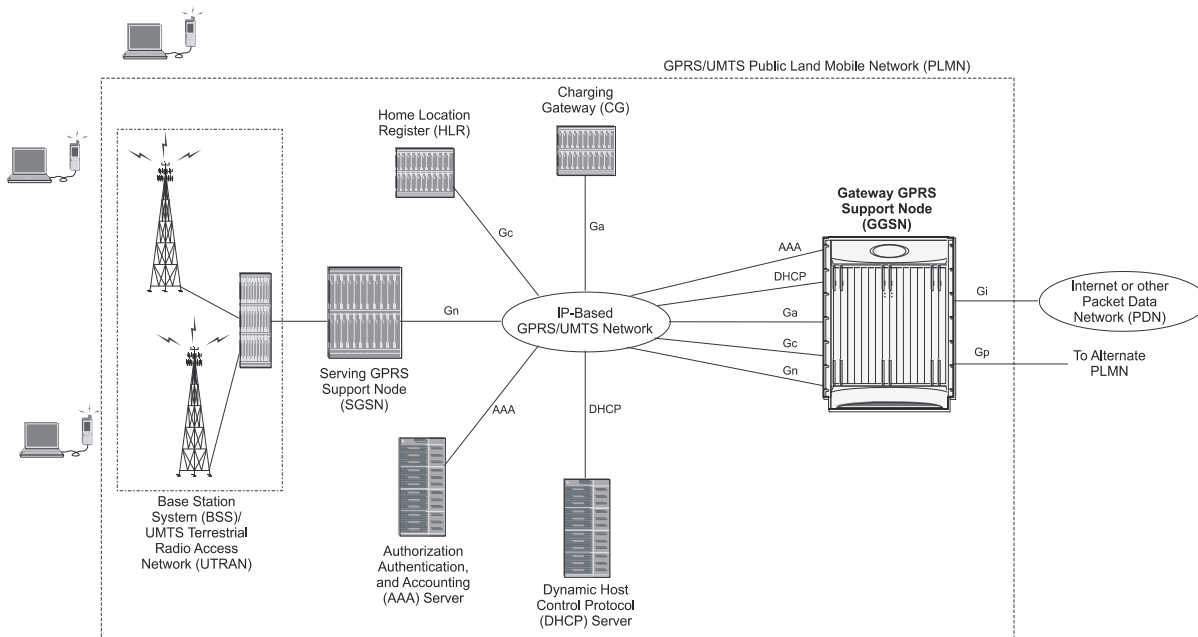
The GGSN works in conjunction with Serving GPRS Support Nodes (SGSNs) within the network to perform the following functions:

- Establish and maintain subscriber Internet Protocol (IP) or Point-to-Point Protocol (PPP) type Packet Data Protocol (PDP) contexts originated by either the mobile or the network
- Provide charging detail records (CDRs) to the charging gateway (CG, also known as the Charging Gateway Function (CGF))
- Route data traffic between the subscriber's Mobile Station (MS) and a Packet Data Networks (PDNs) such as the Internet or an intranet

PDNs are associated with Access Point Names (APNs) configured on the system. Each APN consists of a set of parameters that dictate how subscriber authentication and IP address assignment is to be handled for that APN.

In addition, to providing basic GGSN functionality as described above, the system can be configured to support Mobile IP and/or Proxy Mobile IP data applications in order to provide mobility for subscriber IP PDP contexts. When supporting these services, the system can be configured to either function as a GGSN and Foreign Agent (FA), a stand-alone Home Agent (HA), or a GGSN, FA, and HA simultaneously within the carrier's network.

Figure 1. Basic GPRS/UMTS Network Topology



In accordance with RFC 2002, the FA is responsible for mobile node registration with, and the tunneling of data traffic to/from the subscriber's home network. The HA is also responsible for tunneling traffic, but also maintains subscriber location information in Mobility Binding Records (MBRs).

# Product Specification

This section describes the hardware and software requirement for GGSN service.

The following information is located in this section:

- [Licenses](#)
- [Platform Requirements](#)
- [Operating System Requirements](#)

## Licenses

The GGSN is a licensed Cisco product. Separate session and feature licenses may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

## Platform Requirements

The GGSN service runs on a Cisco® ASR 5x00 Series chassis running StarOS. The chassis can be configured with a variety of components to meet specific network deployment requirements. For additional information, refer to the Installation Guide for the chassis and/or contact your Cisco account representative.

## Operating System Requirements

The GGSN is available for chassis running StarOS™ Release 7.1 or later.

# Network Deployment and Interfaces

This section describes the supported interfaces and deployment scenario of GGSN in GPRS/UMTS network.

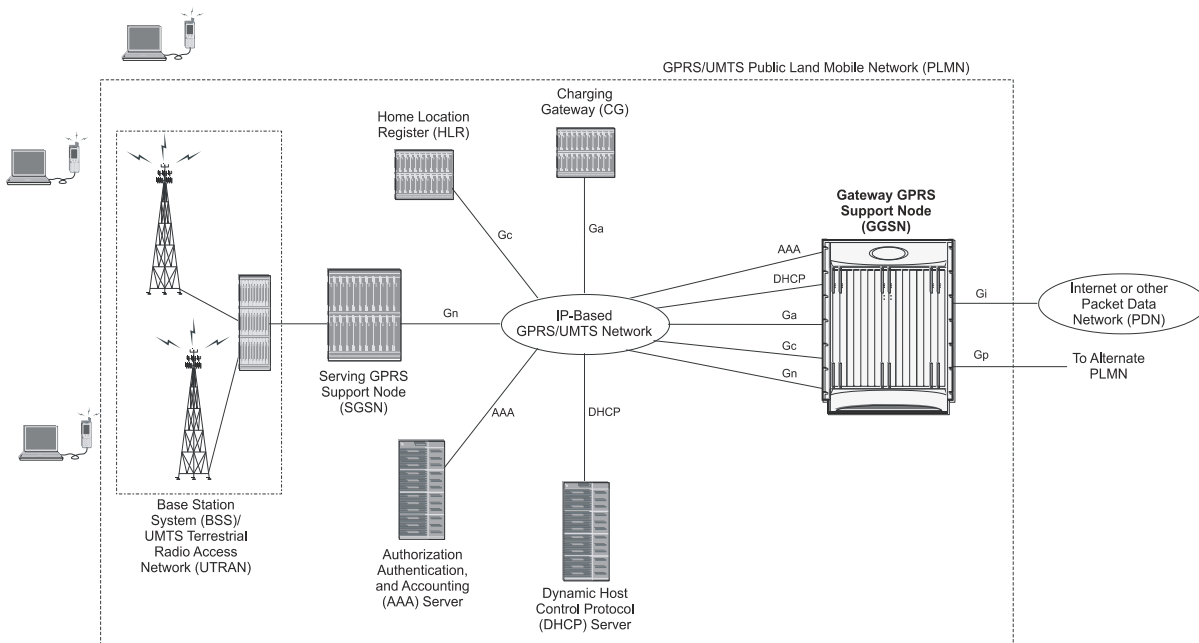
The following information is provided in this section:

- [GGSN in the GPRS/UMTS Data Network](#)
- [Supported Interfaces](#)

## GGSN in the GPRS/UMTS Data Network

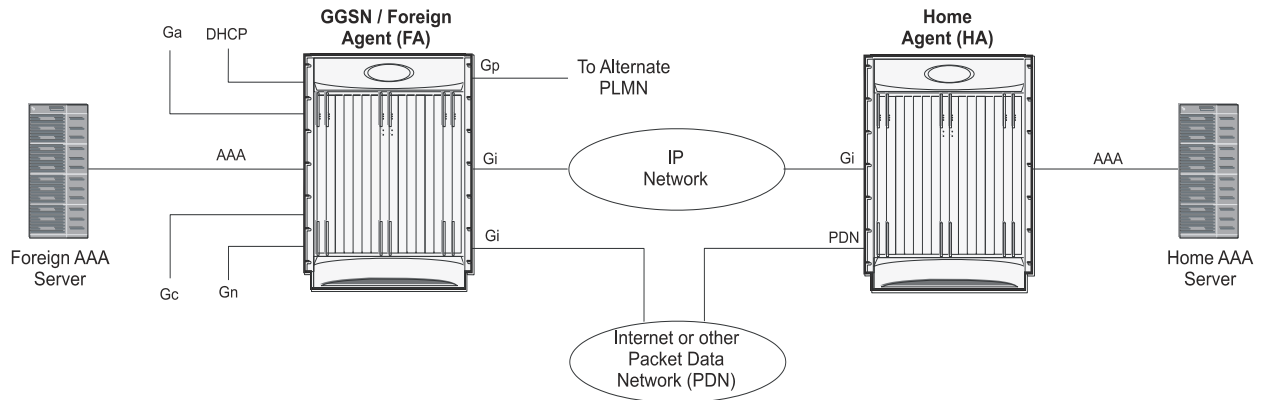
The figures that follow display simplified network views of the GGSN in a GPRS/UMTS network and the system supporting Mobile IP and Proxy Mobile IP function both the GGSN/Foreign Agent (FA) and GGSN/FA/Home Agent (HA) combinations respectively.

**Figure 2. Basic GPRS/UMTS Network Topology**



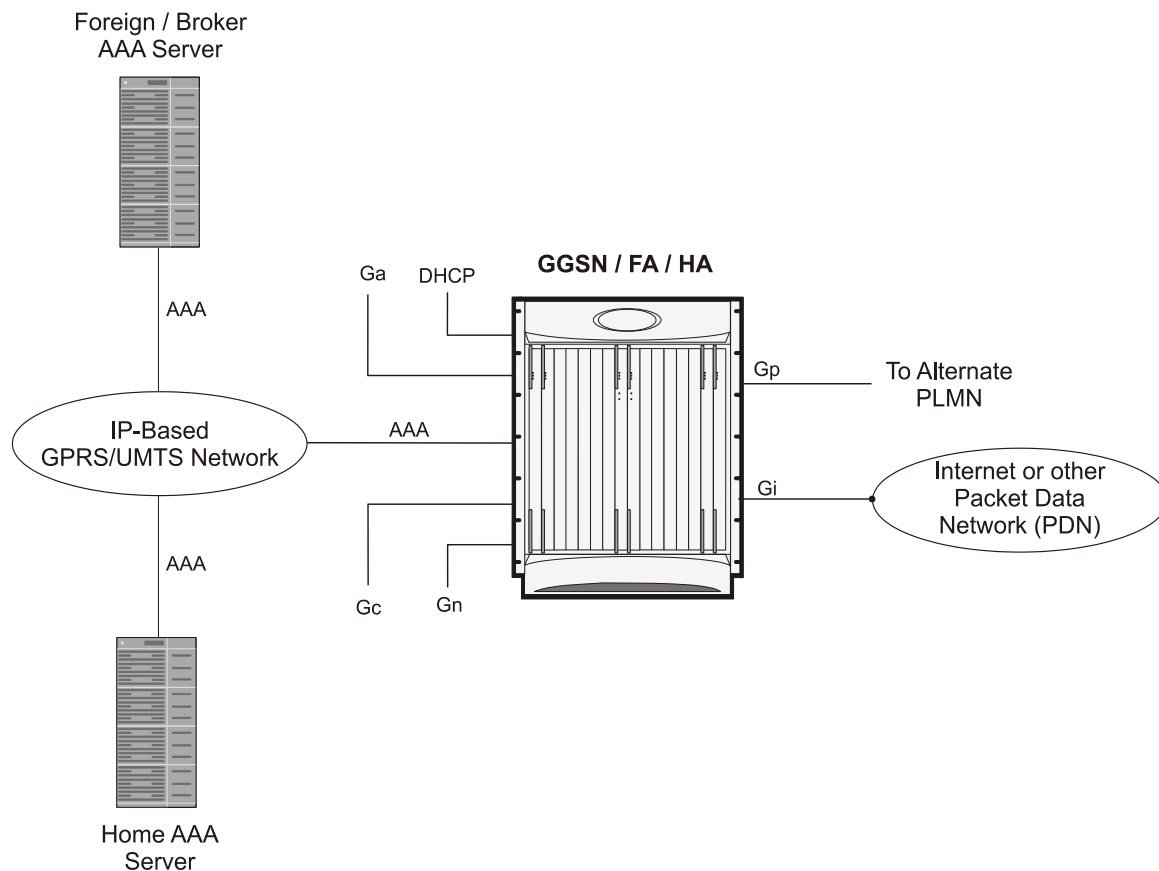
The figures that follow display simplified network views of the GGSN in a GPRS/UMTS network and the system supporting Mobile IP and Proxy Mobile IP function both the GGSN/Foreign Agent (FA) and GGSN/FA/Home Agent (HA) combinations respectively.

**Figure 3. Combined GGSN/FA Deployment for Mobile IP and/or Proxy Mobile IP Support**



The figures that follow display simplified network views of the GGSN in a GPRS/UMTS network and the system supporting Mobile IP and Proxy Mobile IP function both the GGSN/Foreign Agent (FA) and GGSN/FA/Home Agent (HA) combinations respectively.

**Figure 4. Combined GGSN/FA/HA Deployment for Mobile IP and/or Proxy Mobile IP Support**



## Supported Interfaces

In support of both mobile and network originated subscriber PDP contexts, the system GGSN provides the following network interfaces:

- **Gn**: This is the interface used by the GGSN to communicate with SGSNs on the same GPRS/UMTS Public Land Mobile Network (PLMN). This interface serves as both the signaling and data path for establishing and maintaining subscriber PDP contexts.

The GGSN communicates with SGSNs on the PLMN using the GPRS Tunnelling Protocol (GTP). The signaling or control aspect of this protocol is referred to as the GTP Control Plane (GTPC) while the encapsulated user data traffic is referred to as the GTP User Plane (GTPU).

One or more Gn interfaces can be configured per system context.

- **Ga**: This is the interface used by the GGSN to communicate with the Charging Gateway (CG). The charging gateway is responsible for sending GGSN Charging Data Records (G-CDRs) received from the GGSN for each PDP context to the billing system. System supports TCP and UDP as transport layer for this interface.

The GGSN communicates with the CGs on the PLMN using GTP Prime (GTPP).

One or more Ga interfaces can be configured per system context.

- **Gc**: This is the interface used by the GGSN to communicate with the Home Location Register (HLR) via a GTP-to-MAP (Mobile Application Part) protocol convertor. This interface is used for network initiated PDP contexts.

For network initiated PDP contexts, the GGSN will communicate with the protocol convertor using GTP. The convertor, in turn, will communicate with the HLR using MAP over Signaling System 7 (SS7).

One Gc interface can be configured per system context.

- **Gi**: This is the interface used by the GGSN to communicate with Packet Data Networks (PDNs) external to the PLMN. Examples of PDNs are the Internet or corporate intranets.

Inbound packets received on this interface could initiate a network requested PDP context if the intended MS is not currently connected.

For systems configured as a GGSN/FA, this interface is used to communicate with HAs for Mobile IP and Proxy Mobile IP support.

One or more Gi interfaces can be configured per system context. For Mobile IP and Proxy Mobile IP, at least one Gi interface must be configured for each configured FA service. Note that when the system is simultaneously supporting GGSN, FA, and HA services, traffic that would otherwise be routed over the Gi interface is routed inside the chassis.

- **Gp**: This is the interface used by the GGSN to communicate with GPRS Support Nodes (GSNs, e.g. GGSNs and/or SGSNs) on different PLMNs. Within the system, a single interface can serve as both a Gn and a Gp interface.

One or more Gn/Gp interfaces can be configured per system context.

- **AAA**: This is the interface used by the GGSN to communicate with an authorization, authentication, and accounting (AAA) server on the network. The system GGSN communicates with the AAA server using the Remote Authentication Dial In User Service (RADIUS) protocol.

This is an optional interface that can be used by the GGSN for subscriber PDP context authentication and accounting.

- **DHCP**: This is the interface used by the GGSN to communicate with a Dynamic Host Control Protocol (DHCP) Server. The system can be configured as DHCP-Proxy or DHCP Client to provide IP addresses to MS on PDP contexts activation the DHCP server dynamically.



- **Gx:** This is an optional Diameter protocol-based interface over which the GGSN communicates with a Charging Rule Function (CRF) for the provisioning of charging rules that are based on the dynamic analysis of flows used for an IP Multimedia Subsystem (IMS) session. The system provides enhanced support for use of Service Based Local Policy (SBLP) to provision and control the resources used by the IMS subscriber. It also provides Flow based Charging (FBC) mechanism to charge the subscriber dynamically based on content usage.



**Important:** The Gx interface is a license-enabled support. For more information on this support, refer *Gx Interface Support* in this guide.

- **Gy:** This is an optional Diameter protocol-based interface over which the GGSN communicates with a Charging Trigger Function (CTF) server that provides online charging data. Gy interface support provides an online charging interface that works with the ECS deep packet inspection feature. With Gy, customer traffic can be gated and billed in an “online” or “prepaid” style. Both time- and volume-based charging models are supported. In all of these models, differentiated rates can be applied to different services based on shallow or deep packet inspection.



**Important:** This interface is supported through Enhanced Charging Service. For more information on this support, refer *Enhanced Charging Service Administration Guide*.

- **GRE:** This new protocol interface in GGSN platform adds one additional protocol to support mobile users to connect to their enterprise networks: Generic Routing Encapsulation (GRE). GRE Tunneling is a common technique to enable multi-protocol local networks over a single-protocol backbone, to connect non-contiguous networks and allow virtual private networks across WANs. This mechanism encapsulates data packets from one protocol inside a different protocol and transports the data packets unchanged across a foreign network. It is important to note that GRE tunneling does not provide security to the encapsulated protocol, as there is no encryption involved (like IPSEC offers, for example).



**Important:** The GRE protocol interface is a license-enabled support. For more information on this support, refer *GRE Protocol Interface Support* in this guide.

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

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


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


The S6b interface on the P-GW or GGSN can be manually disabled to stop all message traffic to the 3GPP AAA during overload conditions. When the interface is disabled, the system uses locally configured APN-specific parameters including: Framed-Pool, Framed-IPv6-Pool, Idle-Timeout, Charging-Gateway-Function-Host, Server-Name (P-CSCF FQDN). This manual method is used when the HSS/3GPP AAA is in overload condition to allow the application to recover and mitigate the impact to subscribers

Release 12.3 onwards, the IPv6 address reporting through Authorization-Authentication-Request (AAR) towards the S6b interface is no longer a default feature. It is now configurable through the command line interface.

Another enhancement on S6b interface support is the new S6b Retry-and-Continue functionality that creates an automatic trigger in the GGSN and P-GW to use the locally configured APN profile upon receipt of any uniquely defined Diameter error code on the S6b interface for an Authorization-Authentication-Request (AAR) only. This procedure would be utilized in cases where a protocol, transient, or permanent error code is returned from the both the primary and secondary AAA to the GGSN or P-GW. This behavior is only applicable to the aaa-custom15 Diameter dictionary.

---


 **Important:** The S6b interface can still be disabled via the CLI per the existing MOPs in the event of a long-term AAA outage

 **Important:** This interface is supported through license-enabled feature. For more information on this support, refer *Common Gateway Access Support* section of this guide.

---

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

---

 **Important:** GGSN Software also supports additional interfaces. For more information on additional interfaces, refer *Features and Functionality - Optional Enhanced Feature Software* section.

---

## Features and Functionality - Base Software

This section describes the features and functions supported by default in base software on GGSN service and do not require any additional licenses.



**Important:** To configure the basic service and functionality on the system for GGSN service, refer configuration examples provide in *GGSN Administration Guide*.

This section describes following features:

- 16,000 SGSN Support
- AAA Server Groups
- Access Control List Support
- ANSI T1.276 Compliance
- APN Support
- Bulk Statistics Support
- Direct Tunnel Support
- DHCP Support
- DSCP Marking
- Framed-Route Attribute Support
- Generic Corporate APN
- GnGp Handoff Support
- GTPP Support
- Host Route Advertisement
- IP Policy Forwarding
- IP Header Compression - Van Jacobson
- IPv6 Support
- Management System Overview
- MPLS Forwarding with LDP
- Overlapping IP Address Pool Support
- Per APN Configuration to Swap out Gn to Gi APN in CDRs
- Port Insensitive Rule for Enhanced Charging Service
- Quality of Service Support
- RADIUS Support
- PDP Context Support
- RADIUS VLAN Support
- Routing Protocol Support
- Subscriber Session Trace Support

- [Support of Charging Characteristics Provided by AAA Server](#)
- [Support of all GGSN generated causes for partial G-CDR closure](#)
- [Threshold Crossing Alerts \(TCA\) Support](#)

## 16,000 SGSN Support

With growing roaming agreements, many more GPRS/UMTS networks support certain APNs and therefore the number of SGSNs that could connect to the GGSN increases. This feature increases the number of connected SGSNs thereby allowing a single GGSN service to support a much larger roaming network.

The GGSN service supports a maximum of 16,000 SGSN IP addresses. The chassis limit for bulk statistics collection is also limit to 16,000. No change in configuration is needed to support this feature.

## AAA Server Groups

Value-added feature to enable VPN service provisioning for enterprise or MVNO customers. Enables each corporate customer to maintain its own AAA servers with its own unique configurable parameters and custom dictionaries.

This feature provides support for up to 800 AAA (RADIUS and Diameter) server groups and 800 NAS IP addresses that can be provisioned within a single context or across the entire chassis. A total of 128 servers can be assigned to an individual server group. Up to 1,600 accounting, authentication and/or mediation servers are supported per chassis and may be distributed across a maximum of 1,000 APNs. This feature also enables the AAA servers to be distributed across multiple APN within the same context.



**Important:** For more information on AAA Server Group configuration, refer *AAA and GTPP Interface Administration and Reference*.

## Access Control List Support

Access Control Lists provide a mechanism for controlling (i.e permitting, denying, redirecting, etc.) packets in and out of the system.

IP access lists, or Access Control Lists (ACLs) as they are commonly referred to, are used to control the flow of packets into and out of the system. They are configured on a per-context basis and consist of “rules” (ACL rules) or filters that control the action taken on packets that match the filter criteria

Once configured, an ACL can be applied to any of the following:

- An individual interface
- All traffic facilitated by a context (known as a policy ACL)
- An individual subscriber
- All subscriber sessions facilitated by a specific context

There are two primary components of an ACL:

- Rule: A single ACL consists of one or more ACL rules. As discussed earlier, the rule is a filter configured to take a specific action on packets matching specific criteria. Up to 128 rules can be configured per ACL.

Each rule specifies the action to take when a packet matches the specifies criteria. This section discusses the rule actions and criteria supported by the system.

- **Rule Order:** A single ACL can consist of multiple rules. Each packet is compared against each of the ACL rules, in the order in which they were entered, until a match is found. Once a match is identified, all subsequent rules are ignored.



**Important:** For more information on Access Control List configuration, refer *IP Access Control List* in *System Administration Guide*.

## ANSI T1.276 Compliance

ANSI T1.276 specifies security measures for Network Elements (NE). In particular it specifies guidelines for password strength, storage, and maintenance security measures.

ANSI T1.276 specifies several measures for password security.

These measures include:

- Password strength guidelines
- Password storage guidelines for network elements
- Password maintenance, e.g. periodic forced password changes

These measures are applicable to the chassis and the Web Element Manager since both require password authentication. A subset of these guidelines where applicable to each platform will be implemented. A known subset of guidelines, such as certificate authentication, are not applicable to either product. Furthermore, the platforms support a variety of authentication methods such as RADIUS and SSH which are dependent on external elements. ANSI T1.276 compliance in such cases will be the domain of the external element. ANSI T1.276 guidelines will only be implemented for locally configured operators.

## APN Support

The GGSN's Access Point Name (APN) support offers several benefits:

- Extensive parameter configuration flexibility for the APN.
- Creation of subscriber tiers for individual subscribers or sets of subscribers within the APN.
- Virtual APNs to allow differentiated services within a single APN.

Up to 1024 APNs can be configured in the GGSN. An APN may be configured for any type of PDP context, i.e., PPP, IPv4, IPv6 or both IPv4 and IPv6. Many dozens of parameters may be configured independently for each APN.

Here are a few highlights of what may be configured:

- **Accounting:** RADIUS, GTPP or none. Server group to use. Charging characteristics. Interface with mediation servers.
- **Authentication:** Protocol, such as, CHAP or PAP or none. Default username/password. Server group to use. Limit for number of PDP contexts.
- **Enhanced Charging:** Name of rulebase to use, which holds the enhanced charging configuration (e.g., eG-CDR variations, charging rules, prepaid/postpaid options, etc.).
- **IP:** Method for IP address allocation (e.g., local allocation by GGSN, Mobile IP, DHCP, DHCP relay, etc.). IP address ranges, with or without overlapping ranges across APNs.

- **Tunneling:** PPP may be tunneled with L2TP. IPv4 may be tunneled with GRE, IP-in-IP or L2TP. Load-balancing across multiple tunnels. IPv6 is tunneled in IPv4. Additional tunneling techniques, such as, IPsec and VLAN tagging may be selected by the APN, but are configured in the GGSN independently from the APN.
- **QoS:** IPv4 header ToS handling. Traffic rate limits for different 3GPP traffic classes. Mapping of R98 QoS attributes to work around particular handset defections. Dynamic QoS renegotiation (described elsewhere).

After an APN is determined by the GGSN, the subscriber may be authenticated/authorized with an AAA server. The GGSN allows the AAA server to return VSAs (Vendor Specific Attributes) that override any/all of the APN configuration. This allows different subscriber tier profiles to be configured in the AAA server, and passed to the GGSN during subscriber authentication/authorization.

The GGSN's Virtual APN feature allows the carrier to use a single APN to configure differentiated services. The APN that is supplied by the SGSN is evaluated by the GGSN in conjunction with multiple configurable parameters. Then the GGSN selects an APN configuration based on the supplied APN and those configurable parameters. The configurable parameters are: the access gateway IP address, bearer access service name, charging characteristics (CC)-profile index, subscribers within an MSISN range, subscriber's mcc/mnc, whether the subscriber is home/visiting/roaming, subscriber's domain name and the radio access (RAT) type including gen, geran, hspa, eutran, utran, and wlan.



**Important:** For more information on APN configuration, refer *APN Configuration in GGSN Service Configuration*.

## Bulk Statistics Support

The system's support for bulk statistics allows operators to choose to view not only statistics that are of importance to them, but also to configure the format in which it is presented. This simplifies the post-processing of statistical data since it can be formatted to be parsed by external, back-end processors.

When used in conjunction with the Web Element Manager, the data can be parsed, archived, and graphed.

The system can be configured to collect bulk statistics (performance data) and send them to a collection server (called a receiver). Bulk statistics are statistics that are collected in a group. The individual statistics are grouped by schema.

The following schemas are supported for GGSN service:

- **System:** Provides system-level statistics
- **Card:** Provides card-level statistics
- **Port:** Provides port-level statistics
- **FA:** Provides FA service statistics
- **HA:** Provides HA service statistics
- **IP Pool:** Provides IP pool statistics
- **PPP:** Provides Point-to-Point Protocol statistics
- **GTPC:** Provides GPRS Tunneling Protocol - Control message statistics
- **GTPP:** Provides GPRS Tunneling Protocol - Prime message statistics
- **APN:** Provides Access Point Name statistics
- **RADIUS:** Provides per-RADIUS server statistics
- **ECS:** Provides Enhanced Charging Service Statistics

The system supports the configuration of up to 4 sets (primary/secondary) of receivers. Each set can be configured with to collect specific sets of statistics from the various schemas. Statistics can be pulled manually from the system or sent at configured intervals. The bulk statistics are stored on the receiver(s) in files.

The format of the bulk statistic data files can be configured by the user. Users can specify the format of the file name, file headers, and/or footers to include information such as the date, system host name, system uptime, the IP address of the system generating the statistics (available for only for headers and footers), and/or the time that the file was generated.

When the Web Element Manager is used as the receiver, it is capable of further processing the statistics data through XML parsing, archiving, and graphing.

The Bulk Statistics Server component of the Web Element Manager parses collected statistics and stores the information in the PostgreSQL database. If XML file generation and transfer is required, this element generates the XML output and can send it to a Northbound NMS or an alternate bulk statistics server for further processing.

Additionally, if archiving of the collected statistics is desired, the Bulk Statistics server writes the files to an alternative directory on the server. A specific directory can be configured by the administrative user or the default directory can be used. Regardless, the directory can be on a local file system or on an NFS-mounted file system on the Web Element Manager server.

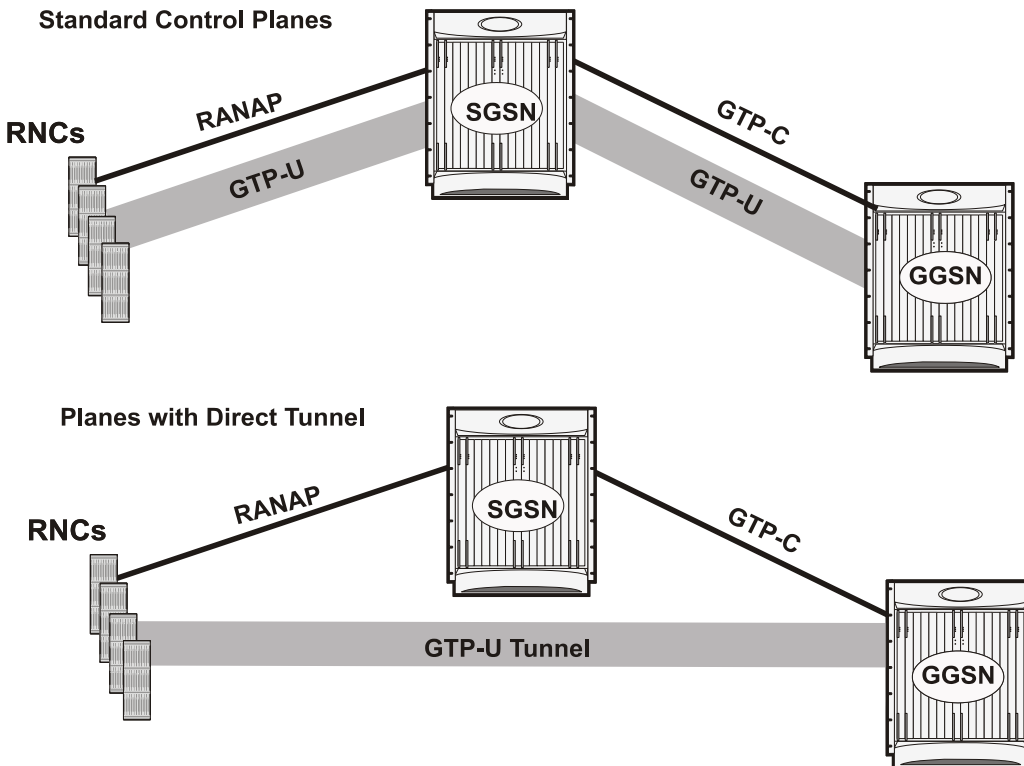
## Direct Tunnel Support

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 typically 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 5. 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 as part of Direct Tunnel deployment. The Cisco 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.

## DHCP Support

Dynamic IP address assignment to subscriber IP PDP contexts using the Dynamic Host Control Protocol as defined by the following standards:

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

As described in the PDP Context Support section of this document, the method by which IP addresses are assigned to a PDP context is configured on an APN-by-APN basis. Each APN template dictates whether it will support static or dynamic addresses.

Dynamically assigned IP addresses for subscriber PDP contexts can be assigned through the use of DHCP.

The system can be configured to support DHCP using either of the following mechanisms:

- **DHCP-proxy:** The system acts as a proxy for client (MS) and initiates the DHCP Discovery Request on behalf of client (MS). Once it receives an allocated IP address from DHCP server in response to DHCP Discovery Request, it assigns the received IP address to the MS. This allocated address must be matched with the an address configured in an IP address pool on the system. This complete procedure is not visible to MS.



- **DHCP-relay:** The system acts as a relay for client (MS) and forwards the DHCP Discovery Request received from client (MS). Once it receives an allocated IP address from DHCP server in response to DHCP Discovery Request, it assigns the received IP address to the MS.



**Important:** For more information on DHCP service configuration, refer *DHCP Configuration* section in *GGSN Service Configuration* chapter.

## DSCP Marking

Provides support for more granular configuration of DSCP marking.

For different Traffic class, the GGSN supports per-GGSN service and per-APN configurable DSCP marking for Uplink and Downlink direction based on Allocation/Retention Priority in addition to the current priorities.

## Framed-Route Attribute Support

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

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

## Generic Corporate APN

Any operator may not be aware of the IP address that a corporation may assign to subscribers through AAA or DHCP and the traffic is sent from the GGSN to the corporation over a tunnel, this feature allows the operator to terminate such users.

Normally the GGSN validates the IP address assigned by RADIUS, however this feature removes the need for this, but does assume that the subscriber traffic is forwarded out of the GGSN through a tunnel.

When the IP address is statically assigned, i.e., either MS provided, RADIUS provided or DHCP provided, the IP address validation is not performed if the address policy is set to disable address validation.

ACL and Policy Group Info processing would still be performed.

Additionally, there is support for Virtual APN selection based on RADIUS VSA returned during Authentication.

The existing Virtual APN selection mechanism is being enhanced to select the Virtual APN based on RADIUS VSA returned during authentication.

The selected V-APN may further require AAA authentication (and accounting) with its own servers.

## GnGp Handoff Support

In LTE deployments, the smooth handover support is required between 3G/2G and LTE networks, and Evolved Packet Core (EPC) is designed to be a common packet core for different access technologies. Since support for seamless

handover across different access technologies is basic requirement for EPC, PGW needs to support handovers as user equipment (UE) moves across different access technologies.

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

### GnGp Handoff in Non-Roaming Scenario

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

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

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

### GnGp Handoff in Roaming Scenario

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



**Important:** For more information on configuration of Gn-Gp Handoff, refer the *Gn-Gp Support Configuration* section of *GGSN Service Configuration Procedures* chapter.

## GTPP Support

Support for the GPRS Tunnelling Protocol Prime (GTPP) in accordance with the following standards:

- **3GPP TS 32.015 v3.12.0 (2003-12):** 3rd Generation Partnership project; Technical Specification Group Services and System Aspects; Telecommunication Management; Charging and billing; GSM call and event data for the Packet Switched (PS) domain (Release 1999) for support of Charging on GGSN
- **3GPP TS 32.215 v5.9.0 (2005-06):** 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Charging management; Charging data description for the Packet Switched (PS) domain (Release 4)
- **3GPP TS 29.060 v7.9.0 (2008-09):** Technical Specification; 3rd Generation Partnership Project; Technical Specification Group Core Network; General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface (Release 6)

The system supports the use of GTPP for PDP context accounting. When the GTPP protocol is used, accounting messages are sent to the Charging Gateways (CGs) over the Ga interface. The Ga interface and GTPP functionality are typically configured within the system's source context. As specified by the standards, a CDR is not generated when a session starts. CDRs are generated according to the interim triggers configured using the charging characteristics

configured for the GGSN, and a CDR is generated when the session ends. For interim accounting, STOP/START pairs are sent based on configured triggers.


GTPP version 2 is always used. However, if version 2 is not supported by the CGF, the system reverts to using GTPP version 1. All subsequent CDRs are always fully-qualified partial CDRs. All CDR fields are R4.

Whether or not the GGSN accepts charging characteristics from the SGSN can be configured on a per-APN basis based on whether the subscriber is visiting, roaming or, home.

By default, the GGSN always accepts the charging characteristics from the SGSN. They must always be provided by the SGSN for GTPv1 requests for primary PDP contexts. If they are not provided for secondary PDP contexts, the GGSN re-uses those from the primary.

If the system is configured to reject the charging characteristics from the SGSN, the GGSN can be configured with its own that can be applied based on the subscriber type (visiting, roaming, or home) at the APN level. GGSN charging characteristics consist of a profile index and behavior settings. The profile indexes specify the criteria for closing accounting records based specific criteria.

---

 **Important:** For more information on GTPP group configuration, refer *GTPP Accounting Configuration* in *GGSN Service Configuration* chapter.

---

## Host Route Advertisement

When subscribers are assigned IP addresses from RADIUS or HLR, yet are allowed to connect to multiple GGSNs through the use of DNS round robin or failover, the IP addresses of the subscribers can be advertised on a per user (host) basis to the Gi network using dynamic routing, thereby providing IP reachability to these users.

IP address pools are configured on the GGSN for many reasons, although one of them is so that the pool subnets can be automatically advertised to the network. These are connected routes and are advertised for all non-tunneling pools.

A configuration **explicit-route-advertise** is provided to the IP pool configuration and when this option is enabled, the subnet(s) of the pool are not added to routing table and routing protocols like OSPF and BGP do not know of these addresses and hence do not advertise the subnet(s).

As calls come up, and addresses from this pool (with the “explicit-route-advertise” flag) are used, the assigned addresses are added to the routing table and these addresses can be advertised by OSPF or BGP through the network or the “redistribute connected” command.

### Example

A subscriber connecting to GGSN A with an IP address from a pool P1 will be assigned the IP address and the routing domain will be updated with the host route. When a subscriber connects to GGSN B with an IP address from the same pool, the subscriber will be assigned the requested IP address and the routing domain will then learn its host route. When the subscriber disconnects, the route is removed from the routing table and the routing domain is updated.

The explicit-route-advertise option can be applied and removed from the pool at any time and the routing tables are updated automatically.

The overlap and resource pool behavior does not change therefore it does not make sense to configure an overlap/resource pool with the “explicit-route-advertise” option.

## IP Policy Forwarding

IP Policy Forwarding enables the routing of subscriber data traffic to specific destinations based on configuration. This functionality can be implemented in support of enterprise-specific applications (i.e. routing traffic to specific enterprise domains) or for routing traffic to back-end servers for additional processing.

The system can be configured to automatically forward data packets to a predetermined network destination. This can be done in one of three ways:

- **IP Pool-based Next Hop Forwarding** - Forwards data packets based on the IP pool from which a subscriber obtains an IP address.
- **ACL-based Policy Forwarding** - Forwards data packets based on policies defined in Access Control Lists (ACLs) and applied to contexts or interfaces.
- **Subscriber specific Next Hop Forwarding** - Forwards all packets for a specific subscriber.

The simplest way to forward subscriber data is to use IP Pool-based Next Hop Forwarding. An IP pool is configured with the address of a next hop gateway and data packets from all subscribers using the IP pool are forward to that gateway.

Subscriber Next Hop forwarding is also very simple. In the subscriber configuration a nexthop forwarding address is specified and all data packets for that subscriber are forwarded to the specified nexthop destination.

ACL-based Policy Forwarding gives you more control on redirecting data packets. By configuring an Access Control List (ACL) you can forward data packets from a context or an interface by different criteria, such as; source or destination IP address, ICMP type, or TCP/UDP port numbers.

ACLs are applied first. If ACL-based Policy Forwarding and Pool-based Next Hop Forwarding or Subscriber are configured, data packets are first redirected as defined in the ACL, then all remaining data packets are redirected to the next hop gateway defined by the IP pool or subscriber profile.



**Important:** For more information on IP Policy Forwarding configuration, refer *Policy Forwarding* in this guide.

## IP Header Compression - Van Jacobson

Implementing IP header compression provides the following benefits:

- Improves interactive response time
- Allows the use of small packets for bulk data with good line efficiency
- Allows the use of small packets for delay sensitive low data-rate traffic
- Decreases header overhead
- Reduces packet loss rate over lossy links

The system supports the Van Jacobson (VJ) IP header compression algorithms by default for subscriber traffic.

The VJ header compression is supported as per RFC 1144 (CTCP) header compression standard developed by V. Jacobson in 1990. It is commonly known as VJ compression. It describes a basic method for compressing the headers of IPv4/TCP packets to improve performance over low speed serial links.

By default IP header compression using the VJ algorithm is enabled for subscribers. You can also turn off IP header compression for a subscriber.



**Important:** For more information on IP header compression support, refer *IP Header Compression* in this guide.

## IPv6 Support

Native IPv6 support allows for the configuration of interfaces/routes with IPv6 (128 bit) addressing. The increased address space allows for future subscriber growth beyond what is currently possible in IPv4. Native IPv6 support on the Gi interface allows support for packets coming from or destined to a mobile over the Gi interface. IPv6 address assignment is supported from a dynamic or static pool via standard 3GPP attributes. The GGSN can communicate using DIAMETER as the transport protocol for Gx to the AAA. Overlapping address space or resource pools are supported if they are in different VPNs. The VPN subsystem is responsible for the configuration and recovery of IP interfaces and routes. IP resources are grouped into separate routing domains known as contexts. The VPN subsystem creates and maintains each context and the resources associated with them. The existing IPv4 model of interface and route notification will be extended to support IPv6.

This feature allows IPv6 subscribers to connect via the GPRS/UMTS infrastructure in accordance with the following standards:

- RFC 2460: Internet Protocol, Version 6 (IPv6) Specification
- RFC 2461: Neighbor Discovery for IPv6
- RFC 2462: IPv6 Stateless Address Autoconfiguration
- RFC 3314: Recommendations for IPv6 in 3GPP Standards
- RFC 3316: Internet Protocol Version 6 (IPv6) for Some Second and Third Generation Cellular Hosts
- RFC 3056: Connection of IPv6 domains via IPv4 clouds
- 3GPP TS 23.060: General Packet Radio Service (GPRS) Service description
- 3GPP TS 27.060: Mobile Station Supporting Packet Switched Services
- 3GPP TS 29.061: Interworking between the Public Land Mobile Network (PLMN) supporting Packet Based Services and Packet Data Networks (PDN)

IP version 6 is enhanced version of IP version 4 with following modifications:

- Expanded addressing capabilities with 128 bit for address as compared to 32 bits in IPv4.
- Header format simplification
- Improved support of extensions and options
- Flow labeling capability
- Authentication and Privacy capabilities

IPv6 Neighbor Discovery protocol is used to dynamically discover the directly attached devices on IPv6 Interfaces. It facilitates the mapping of MAC addresses to IPv6 Addresses. The GGSN supports a subset of IPv6 Neighbor Discovery as defined by RFC 2461, including the following:

- The GGSN uses IPv6 Neighbor Discovery to learn the Ethernet link-layer addresses of the directly connected next-hop gateway.
- The GGSN supports configuration of the static IPv6 neighbor (next-hop gateway).
- Link-local addresses will be automatically added to Ethernet type interfaces.
- The GGSN performs Unsolicited Neighbor Advertisement on line card switchover.
- The GGSN will reply to neighbor discovery requests for the node's IPv6 addresses.

ICMPv6 is a protocol for IPv6 networks to allow error reporting and check connectivity via echo messages. The GGSN supports a subset of ICMPv6 as defined by [RFC-4443]. The GGSN replies to the link-local, configured IP address, and the all-hosts IP address.

Native IPv6 Routing allows the forwarding of IPv6 packets between IPv6 Networks. The forwarding lookup is based on a longest prefix match of the destination IPv6 address. The GGSN supports configuration of IPv6 routes to directly attached next hops via an IPv6 Interface.

## Management System Overview

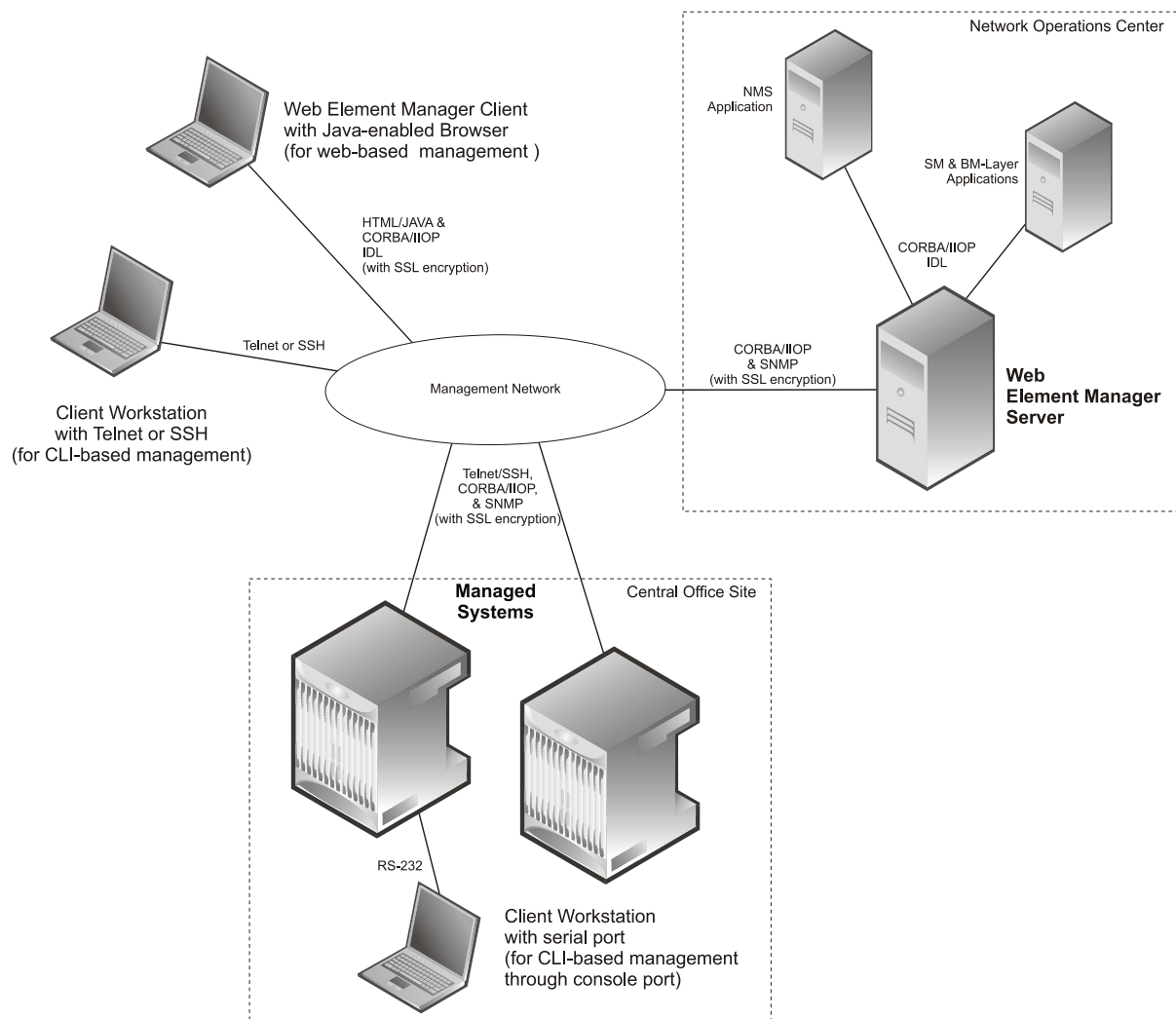
The system's management capabilities are designed around the Telecommunications Management Network (TMN) model for management -- focusing on providing superior quality Network Element (NE) and element management system (Web Element Manager) functions. The system provides element management applications that can easily be integrated, using standards-based protocols (CORBA and SNMPv1, v2), into higher-level management systems -- giving wireless operators the ability to integrate the system into their overall network, service, and business management systems. In addition, all management is performed out-of-band for security and to maintain system performance.

The Operation and Maintenance module of system offers comprehensive management capabilities to the operators and enables them to operate the system more efficiently. There are multiple ways to manage the system either locally or remotely using its out-of-band management interfaces. These include:

- Using the Command Line Interface (CLI)
- Remote login using Telnet, and Secure Shell (SSH) access to CLI through SPIO card's Ethernet management interfaces
- Local login through the Console port on SPIO card using an RS-232 serial connection
- Using the Web Element Manager application
- Supports communications through 10 Base-T, 100 Base-TX, 1000 Base-TX, or 1000
- Base-SX (optical gigabit Ethernet) Ethernet management interfaces on the SPIO
- Client-Server model supports any browser (i.e. Microsoft Internet Explorer v5.0 and above or Netscape v4.7 or above, and others)
- Supports Common Object Request Broker Architecture (CORBA) protocol and Simple Network Management Protocol version 1 (SNMPv1) for fault management
- Provides complete Fault, Configuration, Accounting, Performance, and Security (FCAPS) capabilities
- Can be easily integrated with higher-level network, service, and business layer applications using the Object Management Group's (OMG's) Interface Definition Language (IDL)

The following figure demonstrates these various element management options and how they can be utilized within the wireless carrier network.

Figure 6. Element Management Methods



**Important:** GGSN management functionality is enabled by default for console-based access. For GUI-based management support, refer *Web Element Management System* section.

**Important:** For more information on command line interface based management, refer *Command Line Interface Reference* and *GGSN Administration Guide*.

## MPLS Forwarding with LDP

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

It generates a fixed-length label to attach or bind with the IP packet's header to control the flow and destination of data. The binding of the labels to the IP packets is done by the label distribution protocol (LDP). All the packets in a



forwarding equivalence class (FEC) are forwarded by a label-switching router (LSR) which is also called an MPLS node. The LSR uses the LDP in order to signal its forwarding neighbors and distribute its labels for establishing a label switching path (LSP).

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

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

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

## Overlapping IP Address Pool Support

Overlapping IP Address Pools provides a mechanism for allowing operators to more flexibly support multiple corporate VPN customers with the same private IP address space without the expensive investments in physically separate routers, or expensive configurations using virtual routers.

The system supports two type of overlapping pools: resource and overlap. Resource pools are designed for dynamic assignment only, and use a VPN tunnel, such as a GRE tunnel, to forward and receive the private IP addresses to and from the VPN. Overlapping type pools can be used for both dynamic and static, and use VLANs and a next hop forwarding address to connect to the VPN customer.

To forward downstream traffic to the correct PDP context, the GGSN uses either the GRE tunnel ID, or the VLAN ID to match the packet. When forwarding traffic upstream, the GGSN uses the tunnel and forwarding information in the IP pool configuration, so overlapping pools must be configured in the APN for this feature to be used.

When a PDP context is created, the IP addresses is either assigned from the IP pool, in this case the forwarding rules are also configured into the GGSN at this point. If the address is assigned statically, when the GGSN confirms the IP address from the pool configured in the APN, the forwarding rules are also applied.

The GGSN can scale to as many actual overlapping pools as there are VLAN interfaces per context, and there can be multiple contexts per GGSN, or when using resource then the limit is the number of IP pools. This scalability allows operators, who wish to provide VPN services to customers using the customer's private IP address space, need not be concerned about escalating hardware costs, or complex configurations.



**Important:** For more information on IP pool overlapping configuration, refer *VLANs in System Administration Guide*.

## PDP Context Support

Support for subscriber primary and secondary Packet Data Protocol (PDP) contexts in accordance with the following standards:

- **3GPP TS 23.060 v7.4.0 (2007-9):** 3rd Generation Partnership project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS); Service description (Release 1999) as an additional reference for GPRS/UMTS procedures
- **3GPP TS 29.061 v7.6.0 (2008-09):** 3rd Generation Partnership Project; Technical Specification Group Core Network; Packet Domain; Interworking between the Public Land Mobile Network (PLMN) supporting Packet Based Services and Packet Data Networks (PDN) (Release 4)



PDP context processing is based on the APN that the subscriber is attempting to access. Templates for all of the possible APNs that subscribers will be accessing must be configured within the system. Up to 1024 APNs can be configured on the system.

Each APN template consists of parameters pertaining to how PDP contexts are processed such as the following:

- Type (IPv4, IPv6, IPv4v6, and/or PPP)
- Accounting protocol (GTPP or RADIUS)
- Authentication protocol (CHAP, MSCHAP, PAP, Allow-NOAUTH, IMSI-based, MSISDN-based)
- Charging characteristics (use SGSN-supplied or use configured)
- IP address allocation method (static or dynamic)
- PDP Context timers
- Quality of Service

A total of 11 PDP contexts are supported per subscriber. These could be all primaries, or 1 Primary and 10 secondaries or any combination of primary and secondary. Note that there must be at least one primary PDP context in order for secondaries to come up.

## Per APN Configuration to Swap out Gn to Gi APN in CDRs

In order to allow for better correlation of CDRs with the network or application used by the subscriber, a configuration option has been added to the GGSN replace the Gn APN with the Gi (virtual) APN in emitted G-CDRs.

When virtual APNs are used, the operator can specify via EMS or a configuration command that the Gi APN should be used in the “Access Point Name Network Identifier” field of emitted G-CDRs, instead of the Gn APN.

## Port Insensitive Rule for Enhanced Charging Service

This feature allows a single host or url rule to be applied to two different addresses, one with and one without the port number appended. As adding the port to the address is optional, this means that the number of rules could be halved.

Browser applications can sometimes append the port number to the host or url when sending the host or URL fields. RFC 2616 for example states that port should be appended but if it is omitted then 80 should be assumed.

When configuring rules to define the content, as the web browser may provide the port number, even if it is the default one of 80 for HTTP, then two of each URL are needed.

### Example

```
host = www.w3.org host = www.w3.org:80orhttp url =
http://213.229.187.118:80/chat/c/wel.w.wml http url =
http://213.229.187.118/chat/c/wel.w.wml
```

This feature provides a means to configure the rule such that the traffic is matched irrespective of the presence of a port number.

A new configurable has been added to the rulebase configuration that will ignore the port numbers embedded in the application headers of HTTP, RTSP, SIP, and WSP protocols.

When this feature is enabled, a single rule, such as “host = www.w3.org” would be matched even if the port number is appended and in this case the host field has the value www.w3.org:80, thereby cutting the number of rules needed by up to a half.



**Important:** For more information on enhanced charging service, refer *Enhanced Charging Service Administration Guide*.

## Quality of Service Support

Provides operator control over the prioritization of different types of traffic.

Quality of Service (QoS) support provides internal processing prioritization based on needs, and DiffServ remarking to allow external devices to perform prioritization.



**Important:** The feature described here is internal prioritization and DiffServ remarking for external prioritization. For additional QoS capabilities of the GGSN, refer [Features and Functionality - Optional Enhanced Feature Software](#) section.

External prioritization (i.e., the value to use for the DiffServ marking) is configured for the uplink and downlink directions. In the uplink direction, each APN is configurable for the DiffServ ToS value to use for each of the 3GPP traffic classes. Alternatively, you can configure “pass-through”, whereby the ToS value will pass through unchanged.

In the downlink direction, the ToS value of the subscriber packet is not changed, but you can configure what to use for the ToS value of the outer GTP tunnel. The value for ToS is configurable for each of the 3GPP traffic classes. In addition, the connections between the GGSN and one or more SGSNs can be configured as a “GGSN Service”, and different values for ToS for the same 3GPP traffic class may be configured for different GGSN Services.

## RADIUS Support

Provides a mechanism for performing authorization, authentication, and accounting (AAA) for subscriber PDP contexts based on the following standards:

- RFC-2618, RADIUS Authentication Client MIB, June 1999
- RFC-2620, RADIUS Accounting Client MIB, June 1999
- RFC-2865, Remote Authentication Dial In User Service (RADIUS), June 2000
- RFC-2866, RADIUS Accounting, June 2000
- RFC-2867, RADIUS Accounting Modifications for Tunnel Protocol Support, June 2000
- RFC-2868, RADIUS Attributes for Tunnel Protocol Support, June 2000
- RFC-2869, RADIUS Extensions, June 2000

The Remote Authentication Dial-In User Service (RADIUS) protocol is used to provide AAA functionality for subscriber PDP contexts. (RADIUS accounting is optional since GTPP can also be used.)

Within context contexts configured on the system, there are AAA and RADIUS protocol-specific parameters that can be configured. The RADIUS protocol-specific parameters are further differentiated between RADIUS Authentication server RADIUS Accounting server interaction.

Among the RADIUS parameters that can be configured are:

- **Priority:** Dictates the order in which the servers are used allowing for multiple servers to be configured in a single context.
- **Routing Algorithm:** Dictate the method for selecting among configured servers. The specified algorithm dictates how the system distributes AAA messages across the configured AAA servers for new sessions. Once

a session is established and an AAA server has been selected, all subsequent AAA messages for the session will be delivered to the same server.

In the event that a single server becomes unreachable, the system attempts to communicate with the other servers that are configured. The system also provides configurable parameters that specify how it should behave should all of the RADIUS AAA servers become unreachable.

The system provides an additional level of flexibility by supporting the configuration RADIUS server groups. This functionality allows operators to differentiate AAA services for subscribers based on the APN used to facilitate their PDP context.

In general, 128 AAA Server IP address/port per context can be configured on the system and it selects servers from this list depending on the server selection algorithm (round robin, first server). Instead of having a single list of servers per context, this feature provides the ability to configure multiple server groups. Each server group, in turn, consists of a list of servers.

This feature works in following way:

- All RADIUS authentication/accounting servers configured at the context-level are treated as part of a server group named “default”. This default server group is available to all subscribers in that context through the realm (domain) without any configuration.
- It provides a facility to create “user defined” RADIUS server groups, as many as 399 (excluding “default” server group), within a context. Any of the user defined RADIUS server groups are available for assignment to a subscriber through the APN configuration within that context.

Since the configuration of the APN can specify the RADIUS server group to use as well as IP address pools from which to assign addresses, the system implements a mechanism to support some in-band RADIUS server implementations (i.e. RADIUS servers which are located in the corporate network, and not in the operator's network) where the NAS-IP address is part of the subscriber pool. In these scenarios, the GGSN supports the configuration of the first IP address of the subscriber pool for use as the RADIUS NAS-IP address.



**Important:** For more information on RADIUS AAA configuration, refer *AAA and GTPP Interface Administration and Reference*.

## RADIUS VLAN Support

VPN customers often use private address space which can easily overlap with other customers. The subscriber addresses are supported with overlapping pools which can be configured in the same virtual routing context.

This feature now allows Radius Server and NAS IP addresses to also overlapping without the need to configure separate contexts, thereby simplifying APN and RADIUS configuration and network design.

This feature now allows Radius Server and NAS IP addresses to also overlapping without the need to configure separate contexts, thereby simplifying APN and RADIUS configuration and network design.

This feature supports following scenarios to be defined in the same context:

- Overlapping RADIUS NAS-IP address for various RADIUS server groups representing different APNs.
- Overlapping RADIUS server IP address for various RADIUS servers groups.

Previously, the above scenarios were supported, albeit only when the overlapping addresses were configured in different contexts. Moreover a static route was required in each context for IP connectivity to the RADIUS server.

The new feature utilizes the same concept as overlapping IP pools such that every overlapping NAS-IP address is giving a unique next-hop address which is then bound to an interface that is bound to a unique VLAN, thereby allowing the configuration to exist within the same context.

RADIUS access requests and accounting messages are forwarded to the next hop defined for that NAS-IP and it is then up to the connected router's forward the messages to the RADIUS server. The next hop address determines the interface and VLAN to use. Traffic from the server is identified as belonging to a certain NAS-IP by the port/VLAN combination.

The number of Radius NAS-IP addresses that can be configured is limited by the number of loopback addresses that can be configured.



**Important:** For more information on VLAN support, refer *VLANs* in *System Administration Guide*.

## Routing Protocol Support

The system's support for various routing protocols and routing mechanism provides an efficient mechanism for ensuring the delivery of subscriber data packets.

GGSN node supports Routing Protocol in different way to provide an efficient mechanism for delivery of subscriber data.

The following routing mechanisms and protocols are supported by the system:

- **Static Routes:** The system supports the configuration of static network routes on a per context basis. Network routes are defined by specifying an IP address and mask for the route, the name of the interface in the current context that the route must use, and a next hop IP address.
- **Open Shortest Path First (OSPF) Protocol:** A link-state routing protocol, OSPF is an Interior Gateway Protocol (IGP) that routes IP packets based solely on the destination IP address found in the IP packet header using the shortest path first. IP packets are routed “as is”, meaning they are not encapsulated in any further protocol headers as they transit the network.

Variable length subnetting, areas, and redistribution into and out of OSPF are supported.

OSPF routing is supported in accordance with the following standards:

- RFC-1850, OSPF Version 2 Management Information Base, November 1995
- RFC-2328, OSPF Version 2, April 1998
- RFC-3101 OSPF-NSSA Option, January 2003
- **Border Gateway Protocol version 4 (BGP-4):** The system supports a subset of BGP (RFC-1771, A Border Gateway Protocol 4 (BGP-4)), suitable for eBGP support of multi-homing typically used to support geographically redundant mobile gateways, is supported.

EBGP is supported with multi-hop, route filtering, redistribution, and route maps. The network command is support for manual route advertisement or redistribution.

BGP route policy and path selection is supported by the following means:

- Prefix match based on route access list
- AS path access-list
- Modification of AS path through path prepend
- Origin type
- MED
- Weight

- **Route Policy:** Routing policies modify and redirect routes to and from the system to satisfy specific routing needs. The following methods are used with or without active routing protocols (i.e. static or dynamic routing) to prescribe routing policy:
  - **Route Access Lists:** The basic building block of a routing policy, route access lists filter routes based upon a specified range of IP addresses.
  - **IP Prefix Lists:** A more advanced element of a routing policy. An IP Prefix list filters routes based upon IP prefixes
  - **AS Path Access Lists:** A basic building block used for Border Gateway Protocol (BGP) routing, these lists filter Autonomous System (AS) paths.
- **Route Maps:** Route-maps are used for detailed control over the manipulation of routes during route selection or route advertisement by a routing protocol and in route redistribution between routing protocols. This detailed control is achieved using IP Prefix Lists, Route Access Lists and AS Path Access Lists to specify IP addresses, address ranges, and Autonomous System Paths.
- **Equal Cost Multiple Path (ECMP):** ECMP allows distribution of traffic across multiple routes that have the same cost to the destination. In this manner, throughput load is distributed across multiple path, typically to lessen the burden on any one route and provide redundancy. The mobile gateway supports from four to ten equal-cost paths.



**Important:** For more information on IP Routing configuration, refer *Routing in System Administration Guide*.

## Subscriber Session Trace Support

The Subscriber Level Trace provides a 3GPP standards-based session-level trace function for call debugging and testing new functions and access terminals in an UMTS environment.

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

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

- Management initiation via direct CLI configuration
- Management initiation at AAA with trace activation via authentication response messages over **Gx** reference interface
- Signaling based activation through signaling from subscriber access terminal



**Important:** Once the trace is provisioned it can be provisioned through the access cloud via various signaling interfaces.

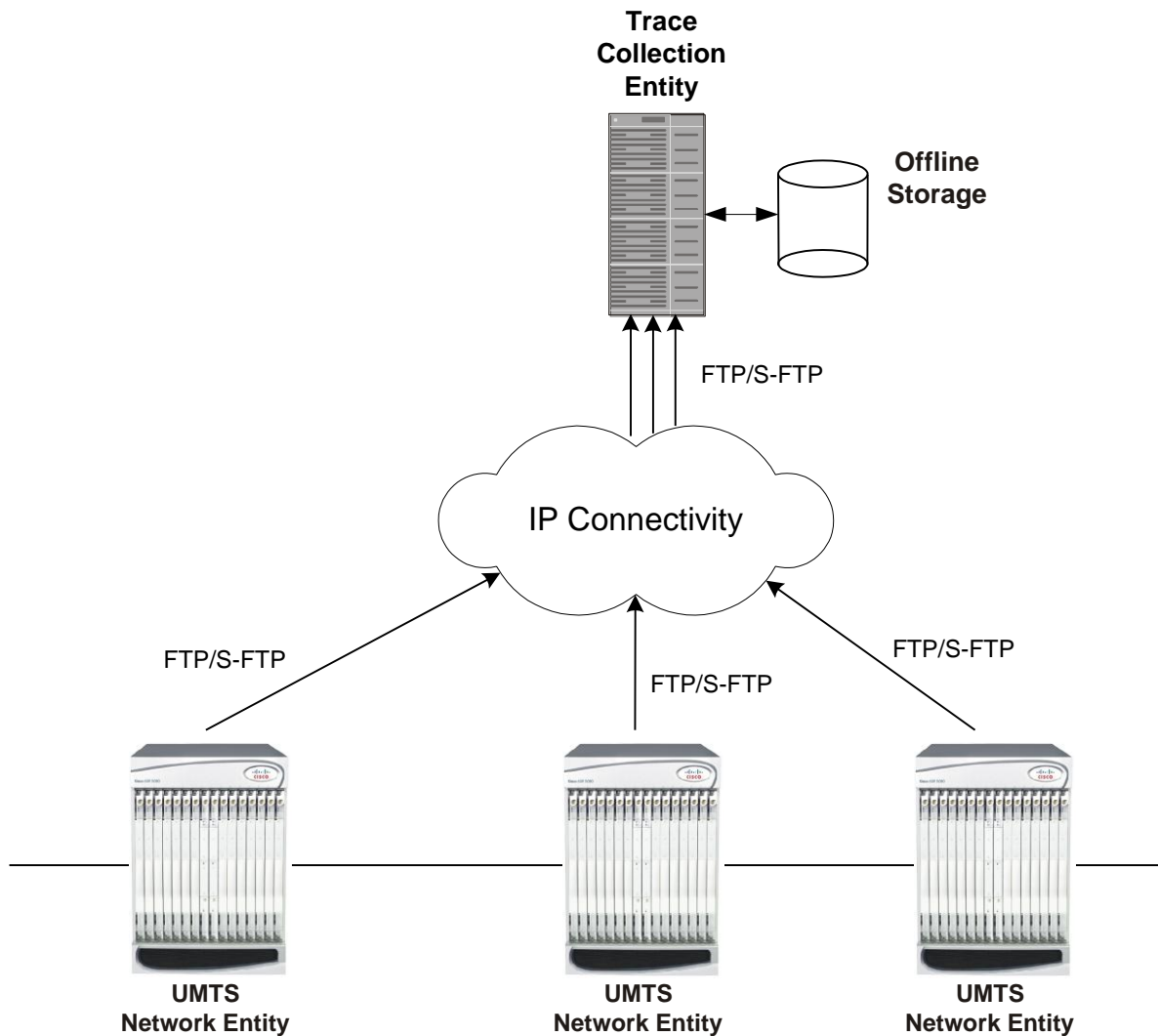
The session level trace function consists of trace activation followed by triggers. The time between the two events is treated much like Lawful Intercept where the UMTS network element buffers the trace activation instructions for the provisioned subscriber in memory using camp-on monitoring. Trace files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



**Important:** Only Maximum Trace Depth is supported in the current release.

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

Figure 7. Session Trace Function and Interfaces



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

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

## Support of Charging Characteristics Provided by AAA Server

This feature provides the ability for operators to apply Charging Characteristics (CC) from the AAA server instead of a hard coded local profile during access authentication.

The RADIUS attribute **3GPP-Chrg-Char** can be used to get the charging characteristics from RADIUS in Access-Accept message. Accepting the RADIUS returned charging characteristic profile must be enabled per APN. The CC profile returned by AAA will override any CC provided by the SGSN, the GGSN or per APN configuration. All 16 profile behaviors can be defined explicitly or the default configuration for that profile is used.

## Support of all GGSN generated causes for partial G-CDR closure

Provides more detailed eG-CDR and/or G-CDR closure causes as per 3GPP TS 32.298.

System handles the GGSN generated causes for partial closure of CDRs. It supports various type of causes including Radio Access Technology Change, MS Time Zone Change, Cell update, inter-PLMN SGSN change, PLMN id change, QoS, Routing-Area update etc.

## Threshold Crossing Alerts (TCA) Support

Thresholding on the system is used to monitor the system for conditions that could potentially cause errors or outage. Typically, these conditions are temporary (i.e high CPU utilization, or packet collisions on a network) and are quickly resolved. However, continuous or large numbers of these error conditions within a specific time interval may be indicative of larger, more severe issues. The purpose of thresholding is to help identify potentially severe conditions so that immediate action can be taken to minimize and/or avoid system downtime.

The system supports Threshold Crossing Alerts for certain key resources such as CPU, memory, IP pool addresses, etc. With this capability, the operator can configure threshold on these resources whereby, should the resource depletion cross the configured threshold, a SNMP Trap would be sent.

The following thresholding models are supported by the system:

- **Alert:** A value is monitored and an alert condition occurs when the value reaches or exceeds the configured high threshold within the specified polling interval. The alert is generated then generated and/or sent at the end of the polling interval.
- **Alarm:** Both high and low threshold are defined for a value. An alarm condition occurs when the value reaches or exceeds the configured high threshold within the specified polling interval. The alert is generated then generated and/or sent at the end of the polling interval.

Thresholding reports conditions using one of the following mechanisms:

- **SNMP traps:** SNMP traps have been created that indicate the condition (high threshold crossing and/or clear) of each of the monitored value.  
Generation of specific traps can be enabled or disabled on the chassis. Ensuring that only important faults get displayed. SNMP traps are supported in both Alert and Alarm modes.
- **Logs:** The system provides a facility called threshold for which active and event logs can be generated. As with other system facilities, logs are generated Log messages pertaining to the condition of a monitored value are generated with a severity level of WARNING  
Logs are supported in both the Alert and the Alarm models.
- **Alarm System:** High threshold alarms generated within the specified polling interval are considered “outstanding” until a the condition no longer exists or a condition clear alarm is generated. “Outstanding”

alarms are reported to the system's alarm subsystem and are viewable through the Alarm Management menu in the Web Element Manager.

The Alarm System is used only in conjunction with the Alarm model.



**Important:** For more information on threshold crossing alert configuration, refer *Thresholding Configuration Guide*.

---



# Features and Functionality - Optional Enhanced Feature Software

This section describes the optional enhanced features and functions for GGSN service.

Each of the following features require the purchase of an additional license to implement the functionality with the GGSN service.

This section describes following features:

- [Common Gateway Access Support](#)
- [Dynamic RADIUS Extensions \(Change of Authorization\)](#)
- [GRE Protocol Interface Support](#)
- [Gx Interface Support](#)
- [Inter-Chassis Session Recovery](#)
- [IP Security \(IPSec\)](#)
- [L2TP LAC Support](#)
- [L2TP LNS Support](#)
- [Lawful Intercept](#)
- [Mobile IP Home and Foreign Agents](#)
- [Mobile IP NAT Traversal](#)
- [Multimedia Broadcast Multicast Services Support](#)
- [Overcharging Protection on Loss of Coverage](#)
- [Proxy Mobile IP](#)
- [Session Persistence](#)
- [Session Recovery Support](#)
- [Traffic Policing and Rate Limiting](#)
- [Web Element Management System](#)

## Common Gateway Access Support

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

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

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

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

## Dynamic RADIUS Extensions (Change of Authorization)

Dynamic RADIUS extension support provide operators with greater control over subscriber PDP contexts by providing the ability to dynamically redirect data traffic, and or disconnect the PDP context.

This functionality is based on the RFC 3576, Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS), July 2003 standard.

The system supports the configuration and use of the following dynamic RADIUS extensions:

- **Change of Authorization:** The system supports CoA messages from the AAA server to change data filters associated with a subscriber session. The CoA request message from the AAA server must contain attributes to identify NAS and the subscriber session and a data filter ID for the data filter to apply to the subscriber session.
- **Disconnect Message:** The DM message is used to disconnect subscriber sessions in the system from a RADIUS server. The DM request message should contain necessary attributes to identify the subscriber session.

The above extensions can be used to dynamically re-direct subscriber PDP contexts to an alternate address for performing functions such as provisioning and/or account set up. This functionality is referred to as Session Redirection, or Hotlining.

Session redirection provides a means to redirect subscriber traffic to an external server by applying ACL rules to the traffic of an existing or a new subscriber session. The destination address and optionally the destination port of TCP/IP or UDP/IP packets from the subscriber are rewritten so the packet is forwarded to the designated redirected address.

Return traffic to the subscriber has the source address and port rewritten to the original values. The redirect ACL may be applied dynamically by means of the Radius Change of Authorization (CoA) extension.



**Important:** For more information on dynamic RADIUS extensions support, refer *CoA, RADIUS, And Session Redirection (Hotlining)* in this guide.

## GRE Protocol Interface Support

GGSN supports GRE generic tunnel interface support in accordance with RFC-2784, Generic Routing Encapsulation (GRE).

GRE protocol functionality adds one additional protocol on the system to support mobile users to connect to their enterprise networks through Generic Routing Encapsulation (GRE).

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

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

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

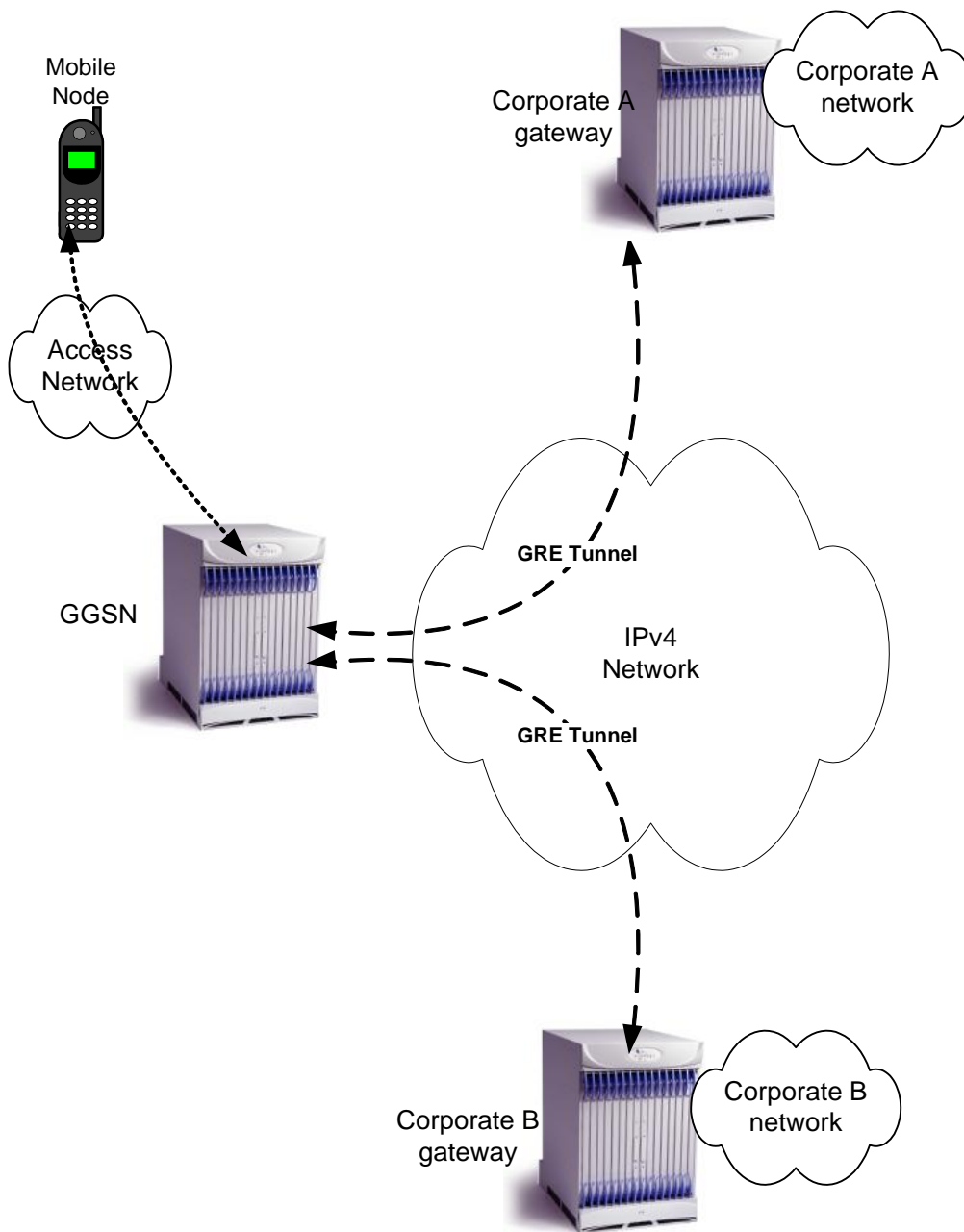
GRE Tunneling consists of three main components:

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

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

The following figure shows a high-level overview of the GRE deployment scenario:

Figure 8. GRE Deployment Scenario



## Gx Interface Support

Gx interface support on the system enables the wireless operator to:

- Implement differentiated service profiles for different subscribers
- Intelligently charge the services accessed depending on the service type and parameters

This interface is particularly suited to control and charge multimedia applications and IMS services. This interface support is compliant to following standards:

- 3GPP TS 23.203 V7.6.0 (2008-03): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Policy and charging control architecture (Release 7)
- 3GPP TS 29.210 V6.2.0 (2005-06): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Charging rule provisioning over Gx interface; (Release 6)
- 3GPP TS 29.212 V7.4.0 (2008-03): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control over Gx reference point (Release 7)
- 3GPP TS 29.213 V7.4.0 (2008-03): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control signalling flows and QoS parameter mapping; (Release 7)
- RFC 3588, Diameter Base Protocol
- RFC 4006, Diameter Credit-Control Application

In addition to the above RFCs and standards IMS authorization partially supports 3GPP TS 29.212 for Policy and Charging Control over Gx reference point functionality.

The goal of the Gx interface is to provide network based QoS control as well as dynamic charging rules on a per bearer basis. The Gx interface is in particular needed to control and charge multimedia applications.

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

The Gx interface is located between the GGSN and the E-PDF / PCRF. It is a Diameter- based interface and provides the functions provided earlier by the Gx and Go interfaces:

- QoS control based on either a token-based or token-less mechanism. In the token-based mechanism, the E-PDF or PCRF dynamically assign network resources to the different bearers used by the subscriber. These resource assignments are transmitted in Tokens carried over the Gx interface. The authorization tokens are allocated by the network (E-PDF/PCRF), hence the network is in full control of the mechanism since it only authorizes resources. The token-less mechanism is for further study.
- Dynamic rules for Flexible Bearer Charging. These dynamic charging rules are carried in the resource assignment tokens and provide 5-tuple type charging rules that enables to implement a specific charging policy for each subscriber bearer. These charging rules will be applied by the FBC function of the GGSN, and produce the appropriate eG-CDRs or the appropriate messages on the Gy interface to the OCS.



**Important:** For more information on Gx interface support, refer *Gx Interface Support* in this guide.

## Inter-Chassis Session Recovery

The chassis provides industry leading carrier class redundancy. The systems protects against all single points of failure (hardware and software) and attempts to recover to an operational state when multiple simultaneous failures occur.

The system provides several levels of system redundancy:

- Under normal N+1 packet processing card hardware redundancy, if a catastrophic packet processing card failure occurs all affected calls are migrated to the standby packet processing card if possible. Calls which cannot be

migrated are gracefully terminated with proper call-termination signaling and accounting records are generated with statistics accurate to the last internal checkpoint

- If the Session Recovery feature is enabled, any total packet processing card failure will cause a packet processing card switchover and all established sessions for supported call-types are recovered without any loss of session.

Even though chassis provides excellent intra-chassis redundancy with these two schemes, certain catastrophic failures which can cause total chassis outages, such as IP routing failures, line-cuts, loss of power, or physical destruction of the chassis, cannot be protected by this scheme. In such cases, the GGSN Inter-Chassis Session Recovery feature provides geographic redundancy between sites. This has the benefit of not only providing enhanced subscriber experience even during catastrophic outages, but can also protect other systems such as the RAN from subscriber re-activation storms.

The Inter-chassis Session Recovery feature allows for continuous call processing without interrupting subscriber services. This is accomplished through the use of redundant chassis. The chassis are configured as primary and backup with one being active and one in recovery mode. A checkpoint duration timer is used to control when subscriber data is sent from the active chassis to the inactive chassis. If the active chassis handling the call traffic goes out of service, the inactive chassis transitions to the active state and continues processing the call traffic without interrupting the subscriber session. The chassis determines which is active through a propriety TCP-based connection called a redundancy link. This link is used to exchange **Hello** messages between the primary and backup chassis and must be maintained for proper system operation.

Interchassis Session Recovery uses following for failur handling and communication:

- **Interchassis Communication:**

Chassis configured to support Interchassis Session Recovery communicate using periodic **Hello** messages. These messages are sent by each chassis to notify the peer of its current state. The **Hello** message contains information about the chassis such as its configuration and priority. A dead interval is used to set a time limit for a **Hello** message to be received from the chassis' peer. If the standby chassis does not receive a **Hello** message from the active chassis within the dead interval, the standby chassis transitions to the active state. In situations where the redundancy link goes out of service, a priority scheme is used to determine which chassis processes the session. The following priority scheme is used:

- router identifier
  - chassis priority
  - SPIO MAC address
- **Checkpoint Message:**

Checkpoint messages are sent from the active chassis to the inactive chassis. Checkpoint messages are sent at specific intervals and contain all the information needed to recreate the sessions on the standby chassis, if that chassis were to become active. Once a session exceeds the checkpoint duration, checkpoint data is collected on the session. The checkpoint parameter determines the amount of time a session must be active before it is included in the checkpoint message.



**Important:** For more information on inter-chassis session recovery support, refer *Interchassis Session Recovery* in *System Administration Guide*.

## IP Security (IPSec)

IP Security provides a mechanism for establishing secure tunnels from mobile subscribers to pre-defined endpoints (i.e. enterprise or home networks) in accordance with the following standards:

- RFC 2401, Security Architecture for the Internet Protocol

- RFC 2402, IP Authentication Header (AH)
- RFC 2406, IP Encapsulating Security Payload (ESP)
- RFC 2409, The Internet Key Exchange (IKE)
- RFC-3193, Securing L2TP using IPSEC, November 2001

IP Security (IPSec) is a suite of protocols that interact with one another to provide secure private communications across IP networks. These protocols allow the system to establish and maintain secure tunnels with peer security gateways.

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

IPSec can be implemented on the system for the following applications:

- **PDN Access:** Subscriber IP traffic is routed over an IPSec tunnel from the system to a secure gateway on the Packet Data Network (PDN) as determined by Access Control List (ACL) criteria.
- **Mobile IP:** Mobile IP control signals and subscriber data is encapsulated in IPSec tunnels that are established between Foreign Agents (FAs) and Home Agents (HAs) over the Pi interfaces.



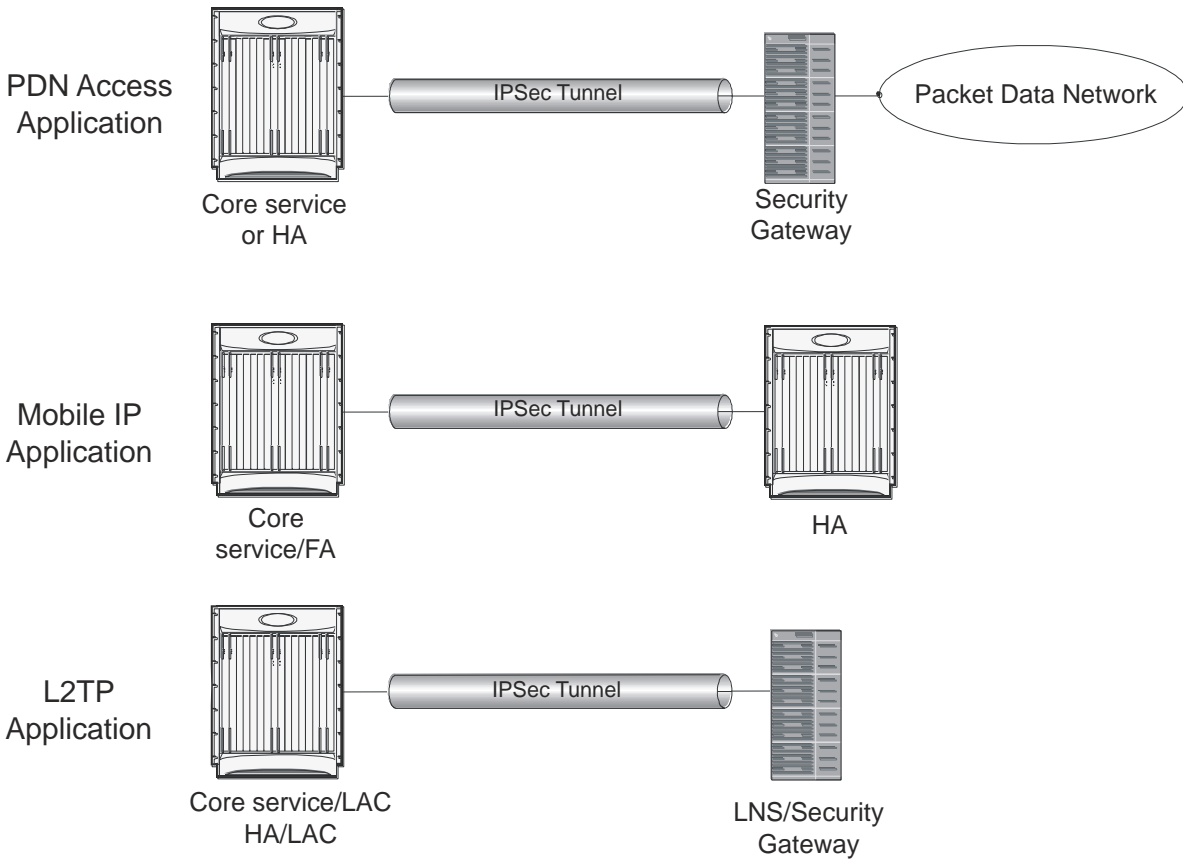
**Important:** Once an IPSec tunnel is established between an FA and HA for a particular subscriber, all new Mobile IP sessions using the same FA and HA are passed over the tunnel regardless of whether or not IPSec is supported for the new subscriber sessions. Data for existing Mobile IP sessions will be unaffected.

---

- **L2TP:** L2TP-encapsulated packets are routed from the system to an LNS/secure gateway over an IPSec tunnel.

The following figure shows a high-level overview of the IPSec application deployment scenario:

Figure 9. IPSec Application Deployment



**Important:** For more information on IPSec support, refer *IP Security* in this guide.

## L2TP LAC Support

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

The use of L2TP in VPN networks is often used as it allows the corporation to have more control over authentication and IP address assignment. An operator may do a first level of authentication, however use PPP to exchange user name and password, and use IPCP to request an address. To support PPP negotiation between the GGSN and the corporation, an L2TP tunnel must be setup in the GGSN running a LAC service.

L2TP establishes L2TP control tunnels between LAC and LNS before tunneling the subscriber PPP connections as L2TP sessions. The LAC service is based on the same architecture as the GGSN and benefits from dynamic resource allocation and distributed message and data processing. This design allows the LAC service to support over 4000 setups per second or a maximum of over 3G of throughput. There can be a maximum up to 65535 sessions in a single tunnel and as many as 500,000 L2TP sessions using 32,000 tunnels per system.

The LAC sessions can also be configured to be redundant, thereby mitigating any impact of hardware or software issues. Tunnel state is preserved by copying the information across processor cards.





**Important:** For more information on this feature support, refer *L2TP Access Concentrator* in this guide.

## L2TP LNS Support

The system configured as a Layer 2 Tunneling Protocol Network Server (LNS) supports the termination secure Virtual Private Network (VPN) tunnels between from L2TP Access Concentrators (LACs).

The LNS service takes advantage of the high performance PPP processing already supported in the system design and is a natural evolution from the LAC. The LNS can be used as a standalone, or running alongside a GGSN service in the same platform, terminating L2TP services in a cost effective and seamless manner.

L2TP establishes L2TP control tunnels between LAC and LNS before tunneling the subscriber PPP connections as L2TP sessions. There can be a maximum of up to 65535 sessions in a single tunnel and up to 500,000 sessions per LNS.

The LNS architecture is similar to the GGSN and utilizes the concept of a de-multiplexer to intelligently assign new L2TP sessions across the available software and hardware resources on the platform without operator intervention.



**Important:** For more information on this feature support, refer *L2TP Network Server* in this guide.

## Lawful Intercept

The system supports the Lawful Interception (LI) of subscriber session information. This functionality provides Telecommunication Service Providers (TSPs) with a mechanism to assist Law Enforcement Agencies (LEAs) in the monitoring of suspicious individuals (referred to as targets) for potential criminal activity.

The following standards were referenced for the system's LI implementation:

- TR-45 Lawfully Authorized Electronic Surveillance TIA/EIA J-STD-025 PN4465 RV 1.7
- 3GPP TS 33.106 V6.1.0 (2004-06): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Lawful Interception requirements (Release 6)
- 3GPP TS 33.107 V6.2.0 (2004-06): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Lawful interception architecture and functions (Release 6)
- 3GPP TS 33.108 V9.0.0 (2009-09): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Handover interface for Lawful Interception (LI) (Release 9)
- Technical Directive: Requirements for implementing statutory telecommunications interception measures (TR TKÜ), Version 4.0

LEAs provide one or more TSPs with court orders or warrants requesting the monitoring of a particular target. The target is identified by information such as their mobile station Integrated Services Digital Network (MSISDN) number, or their International Mobile Subscriber Identification (IMSI) number.

Once the target has been identified, the system, functioning as either a GGSN or HA, serves as an Access Function (AF) and performs monitoring for both new PDP contexts or PDP contexts that are already in progress. While monitoring, the system intercepts and duplicates Content of Communication (CC) and/or Intercept Related Information (IRI) and forwards it to a Delivery Function (DF) over an extensible, proprietary interface. Note that when a target establishes multiple, simultaneous PDP contexts, the system intercepts CC and IRI for each of them. The DF, in turn, delivers the intercepted content to one or more Collection Functions (CFs).

Lawful intercept supports TCP transport on node interfaces along with support for IPv6 address link between chassis and LI server.

On the system with StarOS version 9.0 or later, this feature enhanced to allow 20,000 LI targets to be provisioned as well as monitored.



**Caution:** This capacity improvement impacts performance over various network scenario and in order to reach the full target of 20000 LI targets, it is required that the used platform have at least 12 active packet processing cards installed.



**Important:** For more information on this feature support, refer *Lawful Intercept Configuration Guide*.

## Mobile IP Home and Foreign Agents

Consolidation of GGSN, HA and/or FA services on the same platform eliminates CapEx and OpEx requirements for separate network elements and devices under management. Service integration also enables seamless mobility and inter-technology roaming between 1xEV-DO and UMTS/W-CDMA/GPRS/EDGE radio access networks. This shared configuration also enables common address pools to be applied across all service types. In addition, this combination of collapsed services does not create dependencies for Mobile IP client software on the user access device and consequently does not introduce additional requirements for Mobile IP signaling in the 3GPP radio access network.

This functionality provides the following benefits:

- Timely release of Mobile IP resources at the FA and/or HA
- Accurate accounting
- Timely notification to mobile node of change in service

The system is capable of supporting both GGSN and Mobile IP functions on a single chassis. For Mobile IP applications, the system can be configured to provide the function of a Gateway GPRS Support Node/Foreign Agent (GGSN/FA) and/or a Home Agent (HA).

HA and FA components are defined by RFC 2002 in support of Mobile IP. Mobile IP provides a network-layer solution that allows Mobile Nodes (MNs, i.e. mobile phones, wireless PDAs, and other mobile devices) to receive routed IP packets from their home network while they are connected to any visitor network using their permanent or home IP address. Mobile IP allows mobility in a dynamic method that allows nodes to maintain ongoing communications while changing links as the user traverses the global Internet from various locations outside their home network.

When configured to support HA functionality, the system is capable of supporting following enhanced features:

- **Mobile IP HA Session Rejection/Redirection:** Enables the HA service to either reject new calls or redirect them to another HA when a destination network connection failure is detected. When network connectivity is re-established, the HA service begins to accept calls again in the normal manner. This feature provides the benefit of reducing OpEx through increased operational efficiency and limiting of system downtime.
- **Mobile IP Registration Revocation:** Registration Revocation is a general mechanism whereby the HA providing Mobile IP or Proxy Mobile IP functionality to a mobile node can notify the GGSN/FA of the termination of a binding. Mobile IP Registration Revocation can be triggered at the HA by any of the following:
  - Administrative clearing of calls
  - Session Manager software task outage resulting in the loss of FA sessions (sessions that could not be recovered)
  - Session Idle timer expiry (when configured to send Revocation)
  - Any other condition under which a binding is terminated due to local policy (duplicate IMSI detected, duplicate home address requested)



**Important:** For more information on Mobile IP HA service and FA service configuration, refer *HA Administration Guide* and *GGSN Administration Guide* respectively

## Mobile IP NAT Traversal

This functionality enables converged WiFi-cellular data deployments in which the system is used to concentrate and switch traffic between WiFi hotspots. UDP/IP tunneling enables NAT firewalls in WLAN hotspots to maintain state information for address translation between NATED public address/UDP ports and addresses that are privately assigned for the mobile access device by a local DHCP server.

The Mobile IP protocol does not easily accommodate subscriber mobile nodes that are located behind WLAN or WAN-based NAT devices because it assumes that the addresses of mobile nodes or FA's are globally routable prefixes. However, the mobile node's co-located care of address (CCoA/CoA) is a private address. This presents a problem when remote hosts try to reach the mobile node via the public advertised addresses. The system provides a solution that utilizes UDP tunneling subject to subscriber reservation requests. In this application, the HA uses IP UDP tunneling to reach the mobile subscriber and includes the same private address that was provided in original reservation request in the encapsulated IP payload packet header.



**Important:** For more information on this feature, refer *MIP NAT Traversal* in *System Administration Guide*.

## Multimedia Broadcast Multicast Services Support

Multimedia services are taking on an ever-increasing role in the wireless carriers' plans for an application centric service model. As such, any next generation GGSN platform must be capable of supporting the requirements of multimedia service delivery, including:

- Higher bandwidth requirements of streaming audio and video delivery
- Efficient broadcast and multicast mechanisms, to conserve resources in the RAN

MBMS represents the evolutionary approach to multicast and broadcast service delivery. MBMS uses spectrum resources much more efficiently than Multicast-over-Unicast by optimizing packet replication across all critical components in the bearer path. Thus, services requiring largely uni-directional multicast flows towards the UE are particularly well suited to the MBMS approach. These would include news, event streaming, suitably encoded/compressed cable/radio programs, video-on-demand, multi-chat / group-push-to-talk/video-conferencing sessions with unicast uplink and multicast downlink connections, and other applications.

For MBMS functionality, the system supports the Gmb interface, which is used signal to the BM-SC



**Important:** For more information on this feature, refer *Multicast Broadcast Service* in this guide.

## Overcharging Protection on Loss of Coverage

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

Considering a scenario where a mobile is streaming or downloading very large files from external sources and the mobile goes out of radio coverage. If this download is happening on Background/Interactive traffic class then the GGSN

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

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



**Important:** For more information on this feature, refer *Subscriber Overcharging Protection* in this guide.

## Proxy Mobile IP

Mobility for subscriber sessions is provided through the Mobile IP protocol as defined in RFCs 2002-2005. However, some older Mobile Nodes (MNs) do not support the Mobile IP protocol. The Proxy Mobile IP feature provides a mobility solution for these MNs.

For IP PDP contexts using Proxy Mobile IP, the MN establishes a session with the GGSN as it normally would. However, the GGSN/FA performs Mobile IP operations with an HA (identified by information stored in the subscriber's profile) on behalf of the MN (i.e. the MN is only responsible for maintaining the IP PDP context with the GGSN, no Agent Advertisement messages are communicated with the MN).

The MN is assigned an IP address by either the HA, an AAA server, or on a static-basis. The address is stored in a Mobile Binding Record (MBR) stored on the HA. Therefore, as the MN roams through the service provider's network, each time a hand-off occurs, the MN will continue to use the same IP address stored in the MBR on the HA.

Proxy Mobile IP can be performed on a per-subscriber basis based on information contained in their user profile, or for all subscribers facilitated by a specific APN. In the case of non-transparent IP PDP contexts, attributes returned from the subscriber's profile take precedence over the configuration of the APN.



**Important:** For more information on this feature, refer *Proxy Mobile IP* in this guide.

## Session Persistence



**Important:** Other licenses (i.e. IP Security and L2TP) may be additionally required depending on your network deployment and implementation.

Provides seamless mobility to mobile subscribers as they roam between WLAN and 3G cellular access networks. This type of inter-technology roaming is ordinarily not possible as wireline access networks do not include SGSNs to permit inter-SGSN call hand-offs with cellular access networks.

The Cisco Session Persistence Solution maintains consistent user identities and application transparency for your mobile subscribers as they roam across bearer access networks. This is accomplished through the integration of Home Agent (HA) and GGSN functionality on the wireless access gateway in the packet network and the use of standards-based protocols such as Mobile IP and Mobile IP NAT Traversal. The solution also includes Session Persistence client software that runs on dual-mode WiFi/GPRS/EDGE and/or UMTS/W-CDMA access devices including cellular phones and laptop computers with wireless data cards.

The Session Persistence client is designed to permit Mobile IP tunneling over the applicable underlying network including cellular access connections and cable or XDSL broadband access networks. When the user is attached to a WiFi access network, the Session Persistence client utilizes a Mobile IP Co-located Care of Address Foreign Agent Service (CCoA FA) and establishes a MIP tunnel to the HA service in the platform. This scenario is completely transparent to the GGSN service that operates in the same system. The Mobile IP protocol requires a publicly addressable FA service; however, this is a problem when the mobile subscriber is located behind a NAT firewall. In this case, the NAT firewall has no way of maintaining state to associate the public NATed address with the private address assigned to the user by local DHCP server. Mobile IP NAT Traversal solves this problem by establishing a UDP/IP tunnel between the subscriber access device and Home Agent. The NAT firewall uses the UDP port address to build state for the subscriber session. During this Mobile IP transaction, the HA establishes a mobility binding record for the subscriber session.

When the subscriber roams to a 3GPP cellular access network, it uses the IP address from normal PDP IP context establishment as its new Mobile IP Care of Address to refresh the mobility binding record at the Home Agent. For reduced latency between access hand-offs, it is also possible to utilize a permanent 'always-on' PDP IP context with the IP address maintained in the MIP session persistence client. In this scenario, the mobile access device only needs to re-establish the dormant RAB wireless connection with the 3GPP access network prior to transmitting a new Mobile IP registration.

The system also enables network-provisioned VPNs for Session Persistence applications by permitting use of overlapping address pools on the HA and using various tunneling protocols including IPSEC, Layer 2 Tunneling Protocol (L2TP) and Ethernet IEEE 802.1Q VLANs for separation of subscriber traffic. This application may be further augmented by additional features such as 800 RADIUS Server Groups to permit use of enterprise controlled AAA servers and custom dictionaries.

## Session Recovery Support

The Session Recovery feature 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.

Session recovery is performed by mirroring key software processes (e.g. session manager and AAA manager) within the system. These mirrored processes remain in an idle state (in standby-mode), wherein they perform no processing, until they may be needed in the case of a software failure (e.g. a session manager task aborts). The system spawns new instances of “standby mode” session and AAA managers for each active Control Processor (CP) being used.

Additionally, other key system-level software tasks, such as VPN manager, are performed on a physically separate packet processing card to ensure that a double software fault (e.g. session manager and VPN manager fails at same time on same card) cannot occur. The packet processing card used to host the VPN manager process is in active mode and is reserved by the operating system for this sole use when session recovery is enabled.

The additional hardware resources required for session recovery include a standby System Processor Card (SPC) and a standby packet processing card.

There are following modes of Session Recovery:

- **Task recovery mode:** Wherein one or more session manager failures occur and are recovered without the need to use resources on a standby packet processing card. In this mode, recovery is performed by using the mirrored “standby-mode” session manager task(s) running on active packet processing cards. The “standby-mode” task is renamed, made active, and is then populated using information from other tasks such as AAA manager.
- **Full packet processing card recovery mode:** Used when a packet processing card hardware failure occurs, or when a packet processing card migration failure happens. In this mode, the standby packet processing card is

made active and the “standby-mode” session manager and AAA manager tasks on the newly activated packet processing card perform session recovery.

Session/Call state information is saved in the peer AAA manager task because each AAA manager and session manager task is paired together. These pairs are started on physically different packet processing cards to ensure task recovery.



**Important:** For more information on this feature, refer *Session Recovery* in *System Administration Guide*.

## Traffic Policing and Rate Limiting

Allows the operator to proportion the network and support Service-level Agreements (SLAs) for customers.

The Traffic-Policing/Shaping feature enables configuring and enforcing bandwidth limitations on individual PDP contexts of a particular 3GPP traffic class. Values for traffic classes are defined in 3GPP TS 23.107 and are negotiated with the SGSN during PDP context activation using the values configured for the APN on the GGSN. Configuration and enforcement is done independently on the downlink and the uplink directions for each of the 3GPP traffic classes. Configuration is on a per-APN basis, but may be overridden for individual subscribers or subscriber tiers during RADIUS authentication/authorization.

A Token Bucket Algorithm (a modified trTCM, as specified in RFC2698) is used to implement the Traffic-Policing feature. The algorithm measures the following criteria when determining how to mark a packet:

- **Committed Data Rate (CDR):** The guaranteed rate (in bits per second) at which packets may be transmitted/received for the subscriber during the sampling interval.
- **Peak Data Rate (PDR):** The maximum rate (in bits per second) that packets may be transmitted/received for the subscriber during the sampling interval.
- **Burst-size:** The maximum number of bytes that may be transmitted/received for the subscriber during the sampling interval for both committed (CBS) and peak (PBS) rate conditions. This represents the maximum number of tokens that can be placed in the subscriber's “bucket”. Note that the committed burst size (CBS) equals the peak burst size (PBS) for each subscriber.

Tokens are removed from the subscriber's bucket based on the size of the packets being transmitted/received. Every time a packet arrives, the system determines how many tokens need to be added (returned) to a subscriber's CBS (and PBS) bucket. This value is derived by computing the product of the time difference between incoming packets and the CDR (or PDR). The computed value is then added to the tokens remaining in the subscriber's CBS (or PBS) bucket. The total number of tokens can not be greater than the configured burst-size. If the total number of tokens is greater than the burst-size, the number is set to equal the burst-size. After passing through the Token Bucket Algorithm, the packet is internally classified with a color, as follows:

- There are not enough tokens in the PBS bucket to allow a packet to pass, then the packet is considered to be in violation and is marked “red” and the violation counter is incremented by one.
- There are enough tokens in the PBS bucket to allow a packet to pass, but not in the CBS “bucket”, then the packet is considered to be in excess and is marked “yellow”, the PBS bucket is decremented by the packet size, and the exceed counter is incremented by one.
- There are more tokens present in the CBS bucket than the size of the packet, then the packet is considered as conforming and is marked “green” and the CBS and PBS buckets are decremented by the packet size.

The APN on the GGSN can be configured with actions to take for red and yellow packets. Any of the following actions may be specified:

- **Drop:** The offending packet is discarded.
- **Transmit:** The offending packet is passed.

- **Lower the IP Precedence:** The packet's ToS octet is set to “0”, thus downgrading it to Best Effort, prior to passing the packet.
- **Buffer the Packet:** The packet stored in buffer memory and transmitted to subscriber once traffic flow comes in allowed bandwidth.

Different actions may be specified for red and yellow, as well as for uplink and downlink directions and different 3GPP traffic classes.



**Important:** For more information on this feature, refer *Traffic Policing and Shaping* in this guide.

---

## Web Element Management System

Provides a Graphical User Interface (GUI) for performing Fault, Configuration, Accounting, Performance, and Security (FCAPS) management of the system.

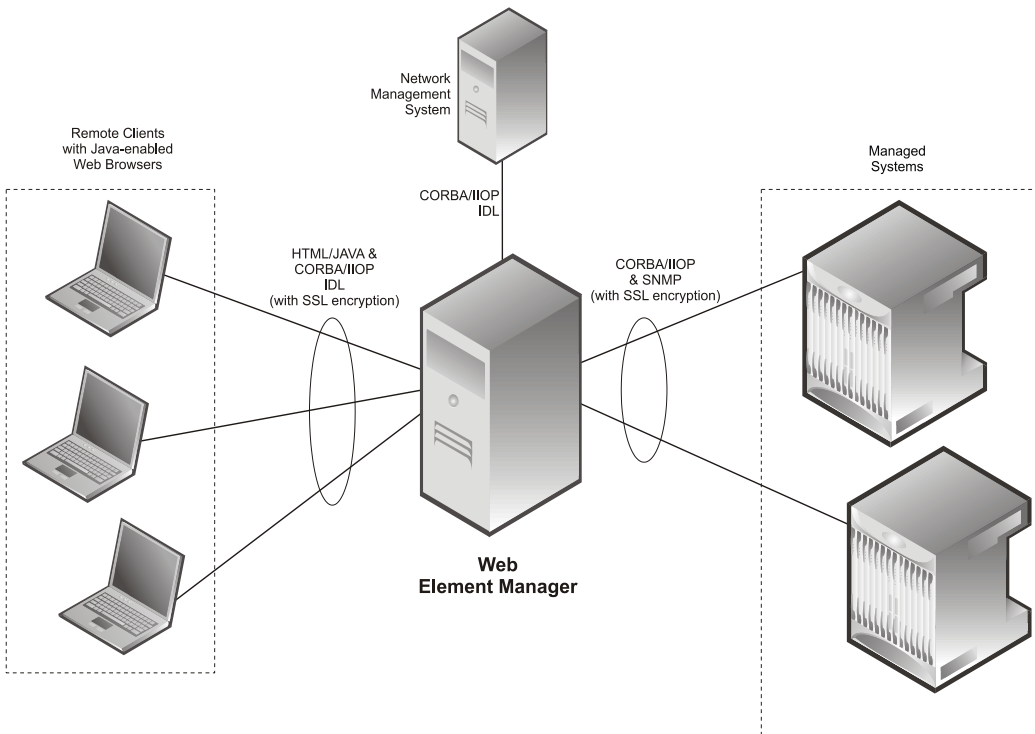
The Web Element Manager is a Common Object Request Broker Architecture (CORBA)-based application that provides complete Fault, Configuration, Accounting, Performance, and Security (FCAPS) management capability for the system.

For maximum flexibility and scalability, the Web Element Manager application implements a client-server architecture. This architecture allows remote clients with Java-enabled web browsers to manage one or more systems via the server component which implements the CORBA interfaces. The server component is fully compatible with the fault-tolerant Sun® Solaris® operating system.

The following figure demonstrates various interfaces between the Cisco Web Element Manager and other network components.



Figure 10. Web Element Manager Network Interfaces



**Important:** For more information on WEM support, refer *WEM Installation and Administration Guide*.



# How GGSN Works

This section provides information on the function of the GGSN in a GPRS/UMTS network and presents call procedure flows for different stages of session setup.

The following topics and procedure flows are included:

- [PDP Context Processing](#)
- [Dynamic IP Address Assignment](#)
- [Subscriber Session Call Flows](#)

## PDP Context Processing

PDP context processing is based on the APN that the subscriber is attempting to access. Templates for all of the possible APNs that subscribers will be accessing must be configured within the system. Up to 1024 APNs can be configured on the system.

Each APN template consists of parameters pertaining to how PDP contexts are processed such as the following:

- **Type:** The system supports IPv4, IPv6, IPv4v6, and PPP PDP contexts. For IPv6 PDP configuration to work, at least one IPv6 interface needs to be configured in the destination context.
- **Accounting protocol:** Support is provided for using either the GTPP or Remote Authentication Dial-In User Service (RADIUS) protocols. In addition, an option is provided to disable accounting if desired.
- **Authentication protocol:** Support is provided for using any of the following:
  - Challenge Handshake Authentication Protocol (CHAP)
  - Microsoft CHAP (MSCHAP)
  - Password Authentication Protocol (PAP)
  - IMSI-based authentication
  - MSISDN-based authentication

In addition, an option is provided to disable authentication if desired.

- **Charging characteristics:** Each APN template can be configured to either accept the charging characteristics it receives from the SGSN for a PDP context or use its own characteristics.
- **IP address allocation method:** IP addresses for PDP contexts can be assigned using one of the following methods:
  - **Statically:** The APN template can be configured to provide support for MS-requested static IP addresses. Additionally, a static address can be configured in a subscriber's profile on an authentication server and allocated upon successful authentication.
  - **Dynamically:** The APN template can be configured to dynamically assign an IP address from locally configured address pools or via a Dynamic Host Control Protocol (DHCP) server. Additional information on dynamic address assignment can be found in the *Dynamic IP Address Assignment* section that follows.



**Important:** Static IP addresses configured in subscriber profiles must also be part of a static IP address pool configured locally on the system.

- **Selection mode:** The MS's right to access the APN can be either verified or unverified. For verified access, the SGSN specifies the APN that should be used. For unverified access, the APN can be specified by either the SGSN or the MS.
- **Timeout:** Absolute and idle session timeout values specify the amount of time that an MS can remain connected.
- **Mobile IP configuration:** Mobile IP requirements, HA address, and other related parameters are configured in the APN template.
- **Proxy Mobile IP support:** Mobile IP support can be enabled for all subscribers facilitated by the APN. Alternatively, it can be enabled for individual subscribers via parameters in their RADIUS or local-user profiles.
- **Quality of Service:** Parameters pertaining to QoS feature support such as for Dynamic Renegotiation, Traffic Policing, and DSCP traffic class.

A total of 11 PDP contexts are supported per subscriber. These could be all primaries, or 1 Primary and 10 secondaries or any combination of primary and secondary. Note that there must be at least one primary PDP context in order for secondaries to come up.

## Dynamic IP Address Assignment

IP addresses for PDP contexts can either be static—an IP address is permanently assigned to the MS—or dynamic—an IP address is temporarily assigned to the MS for the duration of the PDP context.

As previously described in the *PDP Context Processing* section of this chapter, the method by which IP addresses are assigned to a PDP context is configured on an APN-by-APN basis. Each APN template dictates whether it will support static or dynamic addresses. If dynamic addressing is supported, the following methods can be implemented:

- **Local pools:** The system supports the configuration of public or private IP address pools. Addresses can be allocated from these pools as follows:
  - **Public pools:** Provided that dynamic assignment is supported, a parameter in the APN configuration mode specifies the name of the local public address pool to use for PDP contexts facilitated by the APN.
  - **Private pools:** Provided that dynamic assignment is supported, the name of the local private pool can be specified in the subscriber's profile. The receipt of a valid private pool name will override the APN's use of addresses from public pools.
- **Dynamic Host Control Protocol (DHCP):** The system can be configured to use DHCP PDP context address assignment using either of the following mechanisms:
  - **DHCP-proxy:** The system acts as a proxy for client (MS) and initiates the DHCP Discovery Request on behalf of client (MS). Once it receives an allocated IP address from DHCP server in response to DHCP Discovery Request, it assigns the received IP address to the MS. This allocated address must be matched with the an address configured in an IP address pool on the system. This complete procedure is not visible to MS.
  - **DHCP-relay:** The system acts as a relay for client (MS) and forwards the DHCP Discovery Request received from client (MS). Once it receives an allocated IP address from DHCP server in response to DHCP Discovery Request, it assigns the received IP address to the MS.

In addition to the above methods, IP addresses for subscriber Mobile IP sessions are also dynamically assigned by the subscriber's home network upon registration. The GGSN/FA, in turn, provide the assigned address to the mobile station.

## Subscriber Session Call Flows

This section provides information on how GPRS/UMTS subscriber data sessions are processed by the system GGSN. The following data session scenarios are provided:

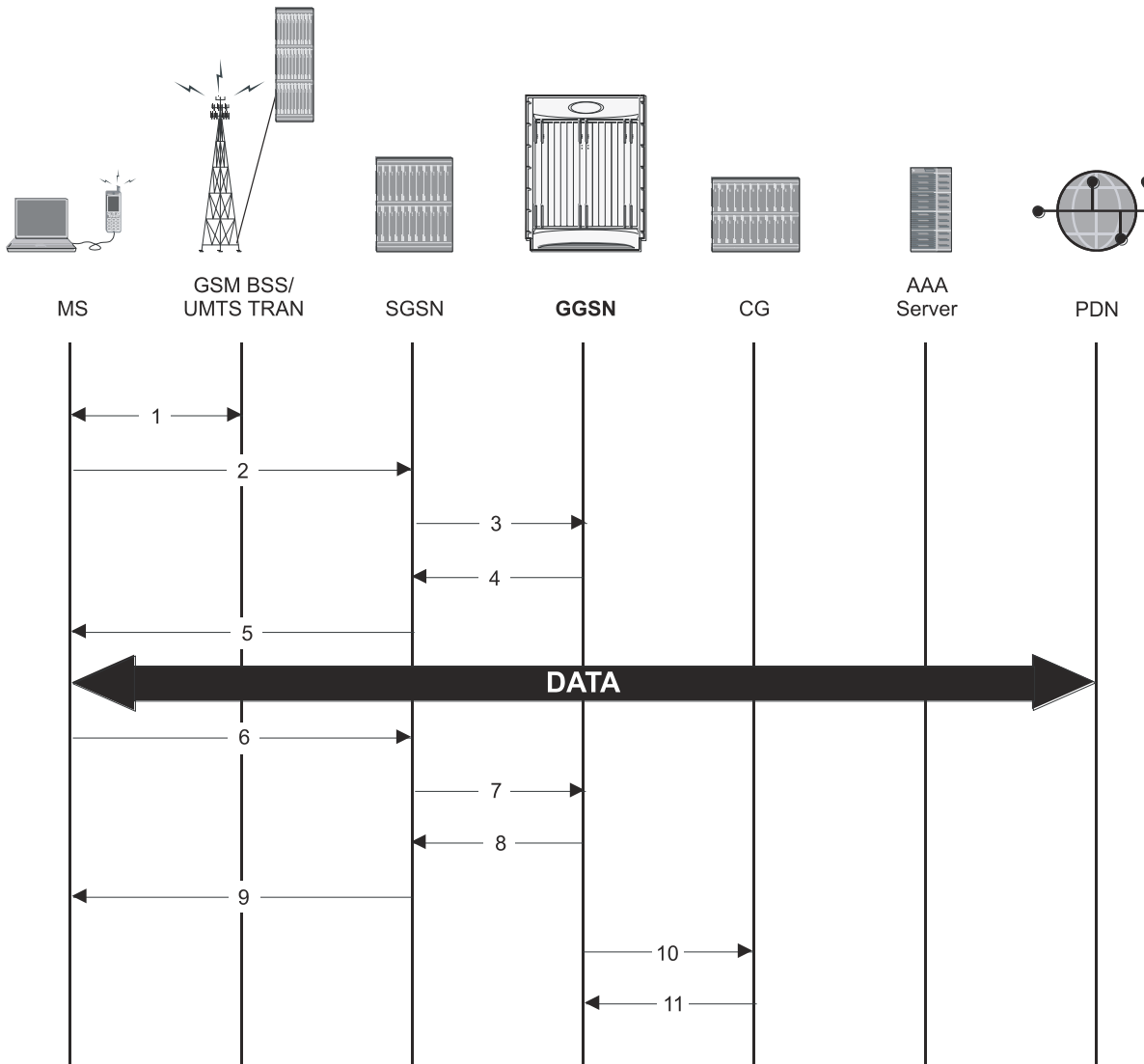
- **Transparent IP:** The subscriber is provided basic access to a PDN without the GGSN authenticating the subscriber. Either a static or dynamic IP address can be assigned to the MS in this scenario.
- **Non-transparent IP:** The GGSN provides subscriber authentication services for the data session. Either a static or dynamic IP address can be assigned to the MS in this scenario.
- **Network-initiated:** An IP Packet Data Unit (PDU) is received by the GGSN from the PDN for a specific subscriber. If configured to support network-initiated sessions, the GGSN, will initiate the process of paging the MS and establishing a PDP context.
- **PPP Direct Access:** The GGSN terminates the subscriber's PPP session and provides subscriber authentication services for the data session. Either a static or dynamic IP address can be assigned to the MS in this scenario.
- **Virtual Dialup Access:** The GGSN functions as an LAC, encapsulates subscriber packets using L2TP, and tunnels them directly to an LNS for processing.
- **Corporate IP VPN Connectivity:** Similar to the Virtual Dialup Access model, however, the GGSN is configured to tunnel subscriber packets to a corporate server using IP-in-IP.
- **Mobile IP:** Subscriber traffic is routed to their home network via a tunnel between the GGSN/FA and an HA. The subscriber's IP PDP context is assigned an IP address from the HA.
- **Proxy Mobile IP:** Provides a mobility solution for subscribers whose Mobile Nodes (MNs) do not support the Mobile IP protocol. The GGSN/FA proxy the Mobile IP tunnel with the HA on behalf of the MS. The subscriber receives an IP address from their home network. As the subscriber roams through the network, the IP address is maintained providing the subscriber with the opportunity to use IP applications that require seamless mobility such as transferring files.
- **IPv6 Stateless Address Auto Configuration:** The mobile station may select any value for the interface identifier portion of the address. The only exception is the interface identifier for the link-local address used by the mobile station. This interface identifier is assigned by the GGSN to avoid any conflict between the mobile station link-local address and the GGSN address. The mobile station uses the interface ID assigned by the GGSN during stateless address auto-configuration procedure (e.g., during the initial router advertisement messages). Once this is over, the mobile can select any interface ID for further communication as long as it does not conflict with the GGSN's interface ID (that the mobile would learn through router advertisement messages from the GGSN).

Additionally, information about the process used by the system to dynamically assign IP addresses to the MS is provided in following sections.

## Transparent Session IP Call Flow

The following figure and the text that follows describe the call flow for a successful transparent data session.

Figure 11. Transparent IP Session Call Flow



1. The Mobile Station (MS) goes through the process of attaching itself to the GPRS/UMTS network.
2. The MS sends an Activate PDP Context Request message that is received by an SGSN. The message contains information about the subscriber such as the Network layer Service Access Point Identifier (NSAPI), PDP Type, PDP Address, Access Point Name (APN), Quality of Service (QoS) requested, and PDP configuration options.
3. The SGSN authenticates the request message and sends a Create PDP Context Request message to a GGSN using the GPRS Tunneling Protocol (GTPC, "C" indicates the control signaling aspect of the protocol). The recipient GGSN is selected based on either the request of the MS or is automatically selected by the SGSN. The message consists of various information elements including: PDP Type, PDP Address, APN, charging characteristics, and Tunnel Endpoint Identifier (TEID, if the PDP Address was static).
4. The GGSN determines if it can facilitate the session (in terms of memory or CPU resources, configuration, etc.) and creates a new entry in its PDP context list and provides a Charging ID for the session.

If the MS required the dynamic assignment of an IP address (i.e., the PDP Address received from the mobile was null), the GGSN will assign one. The IP address assignment methods supported by the system GGSN are described in the *Dynamic IP Address Assignment* section of this guide.

The GGSN replies with an affirmative Create PDP Context Response using GTPC. The response will contain information elements such as the PDP Address representing either the static address requested by the MS or the address assigned by the GGSN, the TEID used to reference PDP Address, and PDP configuration options specified by the GGSN.

5. The SGSN returns an Activate PDP Context Accept response to the MS.

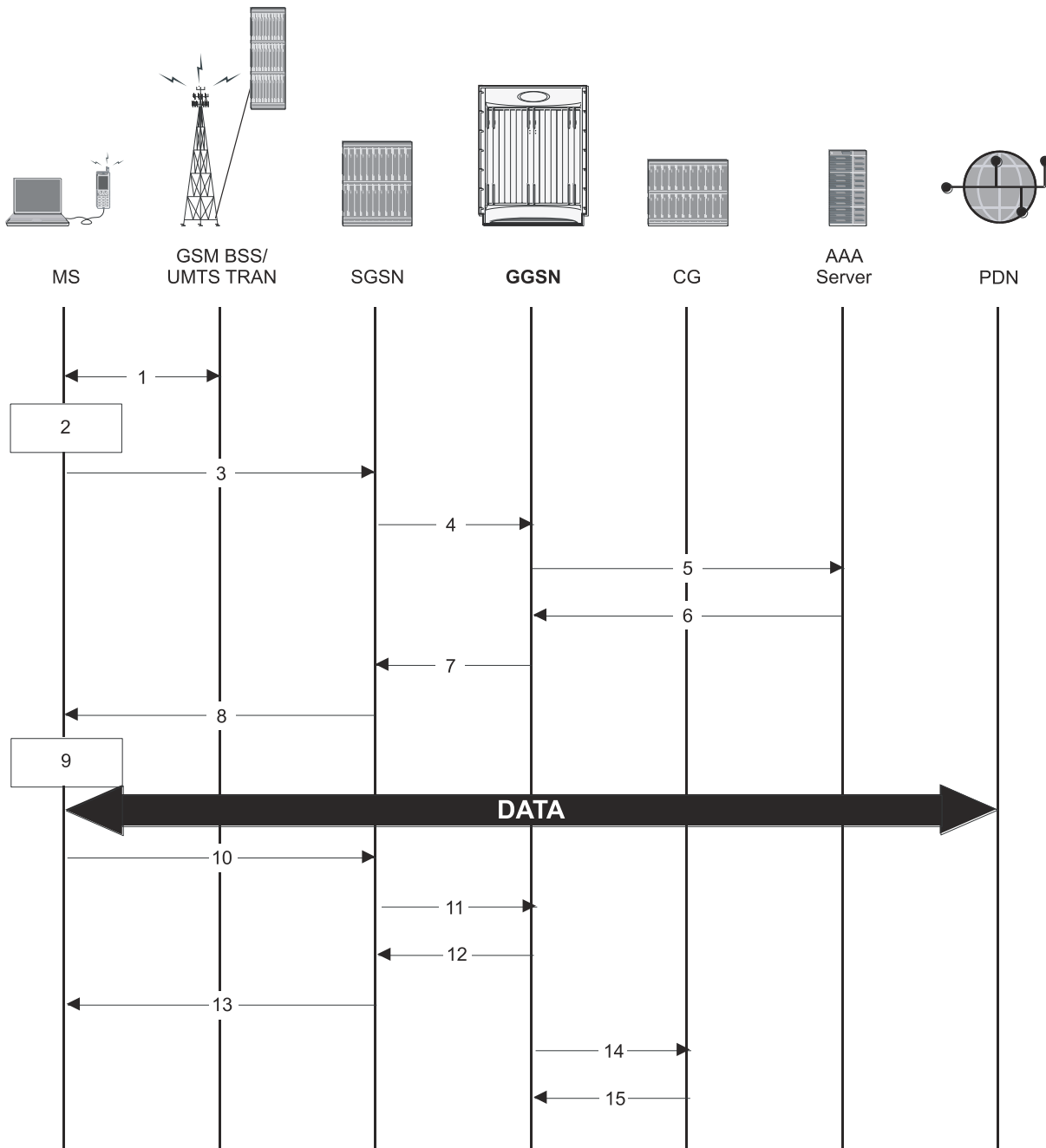
The MS can now send and receive data to or from the PDN until the session is closed or times out. The MS can initiate multiple PDP contexts if desired and supported by the system. Each additional PDP context can share the same IP address or use alternatives.

6. The MS can terminate the data session at any time. To terminate the session, the MS sends a Deactivate PDP Context Request message that is received by the SGSN.
7. The SGSN sends a Delete PDP Context Request message to the GGSN facilitating the data session. The message includes the information elements necessary to identify the PDP context (i.e., TEID, and NSAPI).
8. The GGSN removes the PDP context from memory and returns a Delete PDP Context Response message to the SGSN. If the PDP context was the last associated with a particular dynamically assigned PDP Address, the GGSN will re-claim the IP address for use by subsequent PDP contexts.
9. The SGSN returns a Deactivate PDP Context Accept message to the MS.
10. The GGSN delivers the GGSN Charging Detail Records (G-CDRs) to a Charging Gateway (CG) using GTP Prime (GTPP). Note that, though not shown in this example, the GGSN could optionally be configured to send partial CDRs while the PDP context is active.
11. For each accounting message received from the GGSN, the CG responds with an acknowledgement.

## Non-Transparent IP Session Call Flow

The following figure and the text that follows describe the call flow for a successful non-transparent data session.

Figure 12. Non-Transparent IP Session Call Flow



1. The Mobile Station (MS) goes through the process of attaching itself to the GPRS/UMTS network.
2. The Terminal Equipment (TE) aspect of the MS sends AT commands to the Mobile Terminal (MT) aspect of the MS to place it into PPP mode.

The Link Control Protocol (LCP) is then used to configure the Maximum-Receive Unit size and the authentication protocol (Challenge-Handshake Authentication Protocol (CHAP), Password Authentication Protocol (PAP), or none). If CHAP or PAP is used, the TE will authenticate itself to the MT, which, in turn, stores the authentication information.

Upon successful authentication, the TE sends an Internet Protocol Control Protocol (IPCP) Configure-Request message to the MT. The message will either contain a static IP address to use or request that one be dynamically assigned.

3. The MS sends an Activate PDP Context Request message that is received by an SGSN. The message contains information about the subscriber such as the Network layer Service Access Point Identifier (NSAPI), PDP Type, PDP Address, Access Point Name (APN), Quality of Service (QoS) requested, and PDP configuration options.
4. The SGSN authenticates the request message and sends a Create PDP Context Request message to a GGSN using the GPRS Tunneling Protocol (GTPC, “C” indicates the control signaling aspect of the protocol). The recipient GGSN is selected based on either the request of the MS or is automatically selected by the SGSN. The message consists of various information elements including: PDP Type, PDP Address, APN, charging characteristics, and tunnel endpoint identifier (TEID, if the PDP Address was static).
5. The GGSN determines if it can facilitate the session (in terms of memory or CPU resources, configuration, etc.) and creates a new entry in its PDP context list and provides a Charging ID for the session.

From the APN specified in the message, the GGSN determines whether or not the subscriber is to be authenticated, how an IP address should be assigned if using dynamic allocation, and how to route the session.

If authentication is required, the GGSN attempts to authenticate the subscriber locally against profiles stored in memory or send a RADIUS Access-Request message to an AAA server.

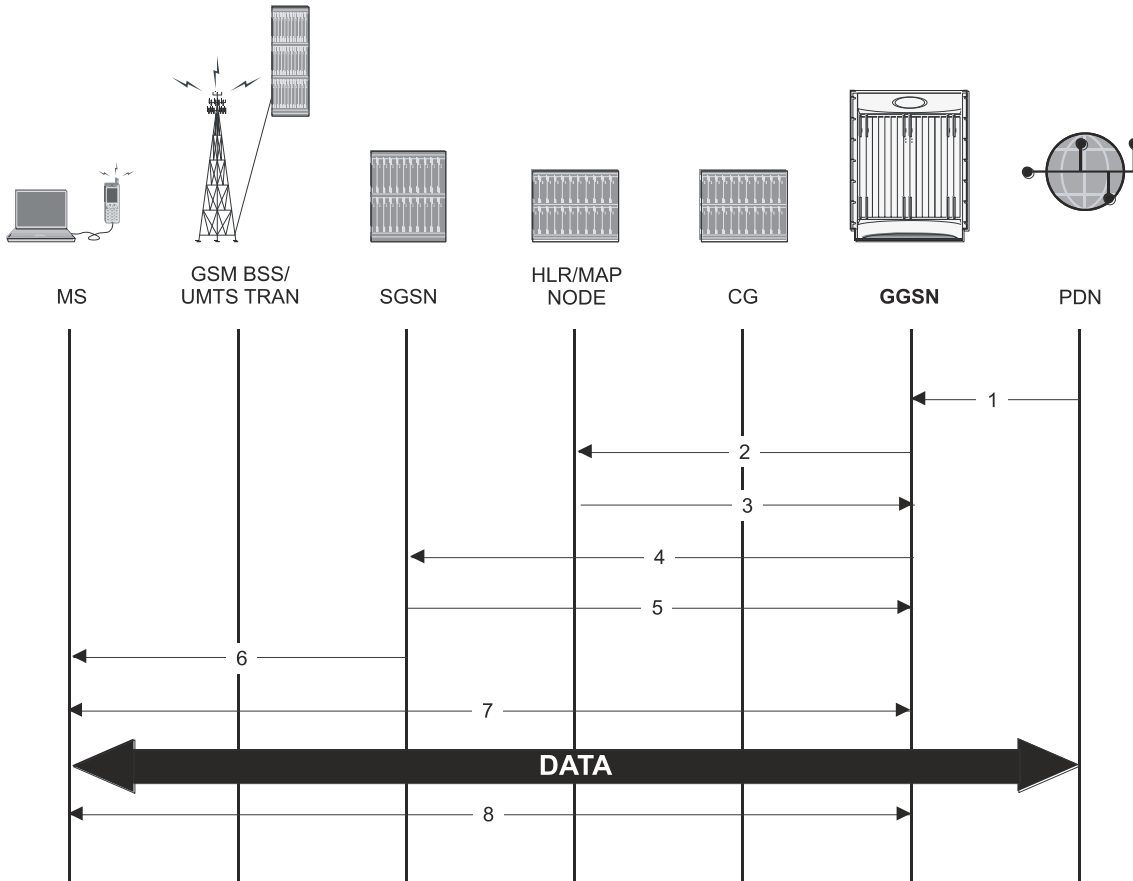
If the MS required the dynamic assignment of an IP address (i.e., the PDP Address received from the mobile was null), the GGSN will assign one. The IP address assignment methods supported by the system GGSN are described in the *Dynamic IP Address Assignment* section of this chapter.
6. If the GGSN authenticated the subscriber to an AAA server, the AAA server responds with a RADIUS Access-Accept message indicating successful authentication.
7. The GGSN replies with an affirmative Create PDP Context Response using GTPC. The response will contain information elements such as the PDP Address representing either the static address requested by the MS or the address assigned by the GGSN, the TEID used to reference PDP Address, and PDP configuration options specified by the GGSN.
8. The SGSN returns an Activate PDP Context Accept message to the MS. The message includes response to the configuration parameters sent in the initial request.
9. The MT, will respond to the TE’s IPCP Config-request with an IPCP Config-Ack message.

The MS can now send and receive data to or from the PDN until the session is closed or times out. The MS can initiate multiple PDP contexts if desired and supported by the system. Each additional PDP context can share the same IP address or use alternatives.
10. The MS can terminate the data session at any time. To terminate the session, the MS sends a Deactivate PDP Context Request message that is received by the SGSN.
11. The SGSN sends a Delete PDP Context Request message to the GGSN facilitating the data session. The message includes the information elements necessary to identify the PDP context (i.e., TEID, and NSAPI).
12. The GGSN removes the PDP context from memory and returns a Delete PDP Context Response message to the SGSN. If the PDP context was the last associated with a particular dynamically assigned PDP Address, the GGSN will re-claim the IP address for use by subsequent PDP contexts.
13. The SGSN returns a Deactivate PDP Context Accept message to the MS.
14. The GGSN delivers the GGSN Charging Detail Records (G-CDRs) to a Charging Gateway (CG) using GTP Prime (GTPP). Note that, though not shown in this example, the GGSN could optionally be configured to send partial CDRs while the PDP context is active.
15. For each accounting message received from the GGSN, the CG responds with an acknowledgement.

## Network-Initiated Session Call Flow

The following figure and the text that follows describe the call flow for a successful network-initiated data session.

Figure 13. Network-initiated Session Call Flow



1. An IP Packet Data Unit (PDU) is received by the GGSN from the PDN. The GGSN determines if it is configured to support network-initiated sessions. If not, it will discard the packet. If so, it will begin the Network-Requested PDP Context Activation procedure.
2. The GGSN may issue a Send Routing Information for GPRS request to the HLR to determine if the MS is reachable. The message includes the MS's International Mobile Subscriber Identity (IMSI).
3. If the MS is reachable, the HLR returns a Send Routing Information for GPRS Ack containing the address of the SGSN currently associated with the MS's IMSI.
4. The GGSN sends a PDU Notification Request message to the SGSN address supplied by the HLR. This message contains the IMSI, PDP Type, PDP Address, and APN associated with the session.
5. The SGSN sends a PDU Notification Response to the GGSN indicating that it will attempt to page the MS requesting that it activate the PDP address indicated in the GGSN's request.
6. The SGSN sends a Request PDP Context Activation message to the MS containing the information supplied by the GGSN.
7. The MS begins the PDP Context Activation procedure as described in *step 2 through step 5* of the *Transparent Session IP Call Flow* section of this chapter.



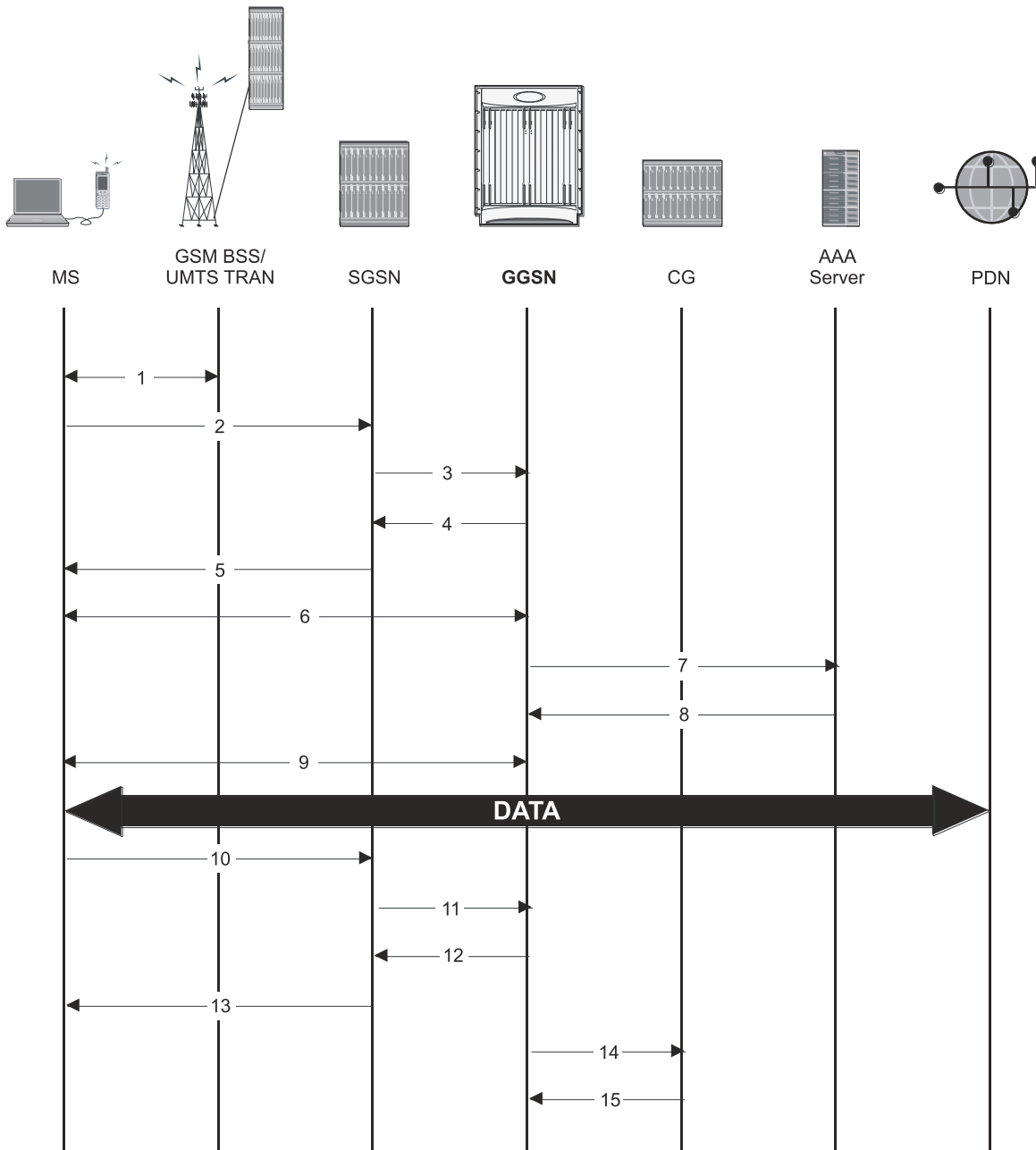
Upon PDP context establishment, the MS can send and receive data to or from the PDN until the session is closed or times out.

8. The MS can terminate the data session at any time. To terminate the session, the MS begins the PDP Context De-Activation procedure as described in *step 6* through *step 11* of the *Transparent Session IP Call Flow* section of this chapter.

## PPP Direct Access Call Flow

The following figure and the text that follows describe the call flow for a successful PPP Direct Access data session.

Figure 14. PPP Direct Access Call Flow



1. The Mobile Station (MS) goes through the process of attaching itself to the GPRS/UMTS network.
2. The MS sends an Activate PDP Context Request message that is received by an SGSN. The message contains information about the subscriber such as the Network layer Service Access Point Identifier (NSAPI), PDP Type, PDP Address, Access Point Name (APN), Quality of Service (QoS) requested, and PDP configuration options.
3. The SGSN authenticates the request message and sends a Create PDP Context Request message to a GGSN using the GPRS Tunneling Protocol (GTPC, "C" indicates the control signaling aspect of the protocol). The

recipient GGSN is automatically selected by the SGSN. The message consists of various information elements including: PDP Type, PDP Address, APN, and charging characteristics.

4. The GGSN determines if it can facilitate the session (in terms of memory or CPU resources, configuration, etc.) and creates a new entry in its PDP context list and provides a Charging ID for the session. It determines that the PDP context type is PPP and based on the APN, what authentication protocol to use and how to perform IP address assignment.

The GGSN replies with an affirmative Create PDP Context Response using GTPC.

5. The SGSN returns an Activate PDP Context Accept response to the MS.
6. The MS and the GGSN negotiate PPP.
7. The GGSN forwards authentication information received from the MS as part of PPP negotiation to the AAA server in the form of an Access-Request.
8. The AAA server authenticates the MS and sends an Access-Accept message to the GGSN.
9. The GGSN assigns an IP address to the MS and completes the PPP negotiation process. More information about IP addressing for PDP contexts is located in the *PDP Context Processing* and *Dynamic IP Address Assignment* sections of this chapter.

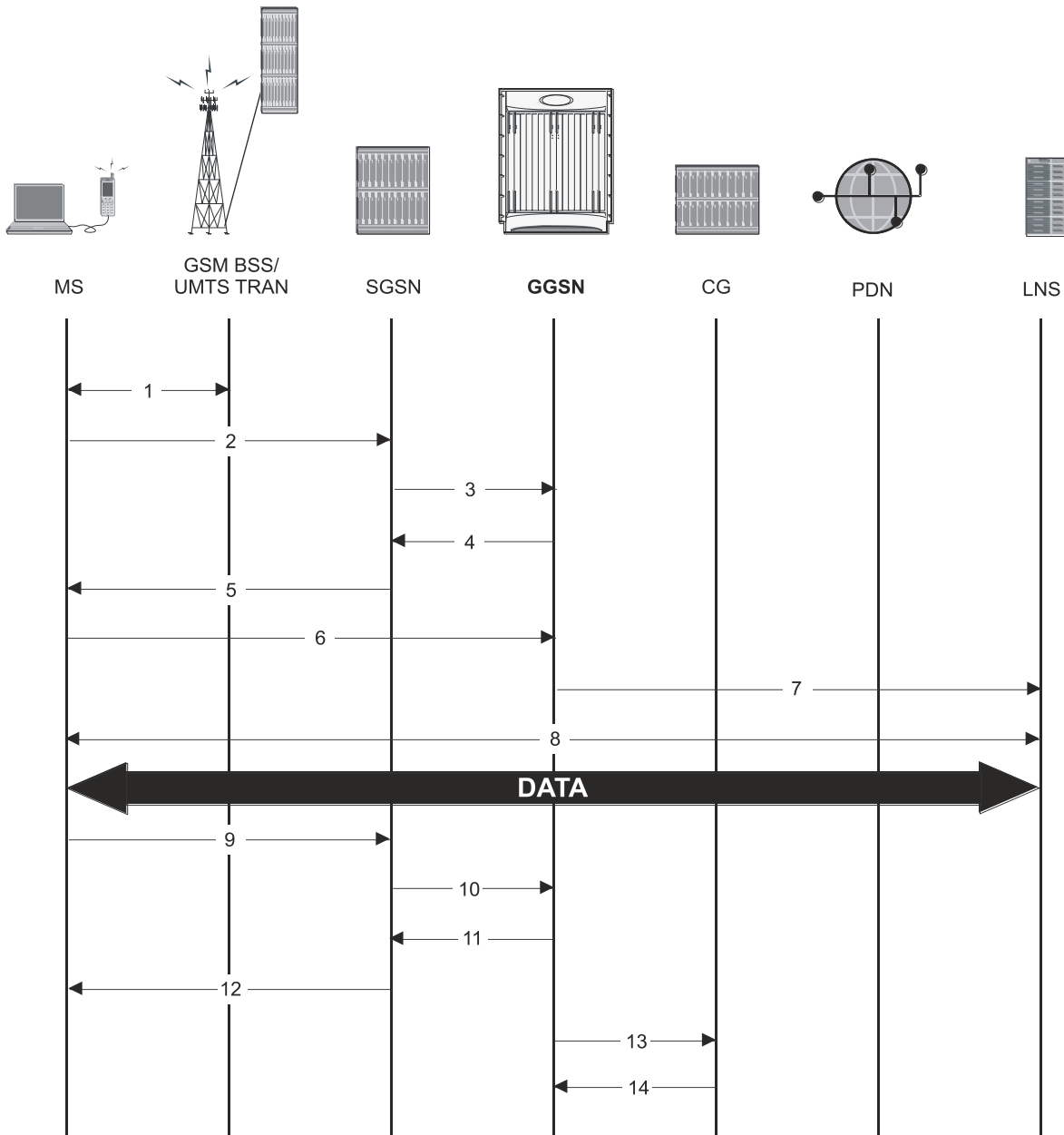
Once the PPP negotiation process is complete, the MS can send and receive data.

10. The MS can terminate the data session at any time. To terminate the session, the MS sends a Deactivate PDP Context Request message that is received by the SGSN.
11. The SGSN sends a Delete PDP Context Request message to the GGSN facilitating the data session. The message includes the information elements necessary to identify the PDP context.
12. The GGSN removes the PDP context from memory and returns a Delete PDP Context Response message to the SGSN. If the PDP context was the last associated with a particular dynamically assigned PDP Address, the GGSN will re-claim the IP address for use by subsequent PDP contexts.
13. The SGSN returns a Deactivate PDP Context Accept message to the MS.
14. The GGSN delivers the GGSN Charging Detail Records (G-CDRs) to a Charging Gateway (CG) using GTP Prime (GTPP). Note that, though not shown in this example, the GGSN could optionally be configured to send partial CDRs while the PDP context is active.
15. For each accounting message received from the GGSN, the CG responds with an acknowledgement.

## Virtual Dialup Access Call Flow

The following figure and the text that follows describe the call flow for a successful VPN Dialup Access data session.

Figure 15. Virtual Dialup Access Call Flow



1. The Mobile Station (MS) goes through the process of attaching itself to the GPRS/UMTS network.
2. The MS sends an Activate PDP Context Request message that is received by an SGSN. The message contains information about the subscriber such as the Network layer Service Access Point Identifier (NSAPI), PDP Type, PDP Address, Access Point Name (APN), Quality of Service (QoS) requested, and PDP configuration options.
3. The SGSN authenticates the request message and sends a Create PDP Context Request message to a GGSN using the GPRS Tunneling Protocol (GTPC, "C" indicates the control signaling aspect of the protocol). The recipient GGSN is automatically selected by the SGSN. The message consists of various information elements including: PDP Type, PDP Address, APN, and charging characteristics.

4. The GGSN determines if it can facilitate the session (in terms of memory or CPU resources, configuration, etc.) and creates a new entry in its PDP context list and provides a Charging ID for the session. It determines the PDP context type and based on the APN, what authentication protocol to use and how to perform IP address assignment.

The GGSN replies with an affirmative Create PDP Context Response using GTPC.

5. The SGSN returns an Activate PDP Context Accept response to the MS.
6. The MS sends packets which are received by the GGSN.
7. The GGSN encapsulates the packets from the MS using L2TP and tunnels them to the LNS.
8. The LNS terminates the tunnel and un-encapsulates the packets.

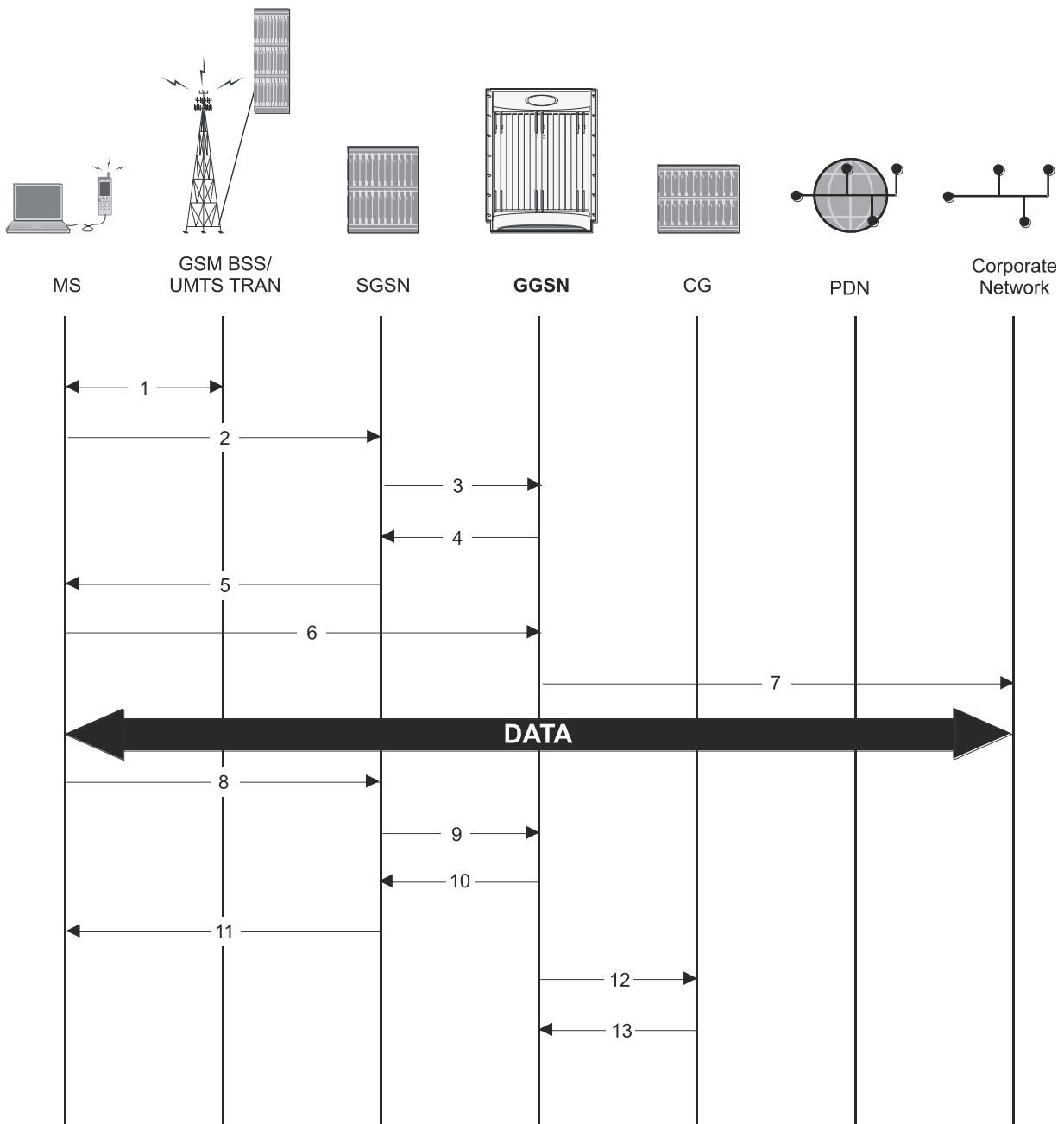
The MS can send and receive data over the L2TP tunnel facilitated by the GGSN.

9. The MS can terminate the data session at any time. To terminate the session, the MS sends a Deactivate PDP Context Request message that is received by the SGSN.
10. The SGSN sends a Delete PDP Context Request message to the GGSN facilitating the data session. The message includes the information elements necessary to identify the PDP context.
11. The GGSN removes the PDP context from memory and returns a Delete PDP Context Response message to the SGSN. If the PDP context was the last associated with a particular dynamically assigned PDP Address, the GGSN will re-claim the IP address for use by subsequent PDP contexts.
12. The SGSN returns a Deactivate PDP Context Accept message to the MS.
13. The GGSN delivers the GGSN Charging Detail Records (G-CDRs) to a Charging Gateway (CG) using GTP Prime (GTPP). Note that, though not shown in this example, the GGSN could optionally be configured to send partial CDRs while the PDP context is active.
14. For each accounting message received from the GGSN, the CG responds with an acknowledgement.

## Corporate IP VPN Connectivity Call Flow

The following figure and the text that follows describe the call flow for a successful Corporate IP Connectivity data session.

Figure 16. Corporate IP VPN Connectivity Call Flow



1. The Mobile Station (MS) goes through the process of attaching itself to the GPRS/UMTS network.
2. The MS sends an Activate PDP Context Request message that is received by an SGSN. The message contains information about the subscriber such as the Network layer Service Access Point Identifier (NSAPI), PDP Type, PDP Address, Access Point Name (APN), Quality of Service (QoS) requested, and PDP configuration options.
3. The SGSN authenticates the request message and sends a Create PDP Context Request message to a GGSN using the GPRS Tunneling Protocol (GTPC, "C" indicates the control signaling aspect of the protocol). The

recipient GGSN is automatically selected by the SGSN. The message consists of various information elements including: PDP Type, PDP Address, APN, and charging characteristics.

4. The GGSN determines if it can facilitate the session (in terms of memory or CPU resources, configuration, etc.) and creates a new entry in its PDP context list and provides a Charging ID for the session. It determines the PDP context type and based on the APN, what authentication protocol to use and how to perform IP address assignment.

If the MS required the dynamic assignment of an IP address (i.e., the PDP Address received from the mobile was null), the GGSN will assign one. The IP address assignment methods supported by the system GGSN are described in the *Dynamic IP Address Assignment* section of this chapter.

The GGSN replies with an affirmative Create PDP Context Response using GTPC.

5. The SGSN returns an Activate PDP Context Accept response to the MS.
6. The MS sends IP packets which are received by the GGSN.
7. The GGSN encapsulates the IP packets from the MS using IP-in-IP and tunnels them to the subscriber's corporate network.

All data sent and received by the MS over the IP-in-IP tunnel facilitated by the GGSN.

8. The MS can terminate the data session at any time. To terminate the session, the MS sends a Deactivate PDP Context Request message that is received by the SGSN.
9. The SGSN sends a Delete PDP Context Request message to the GGSN facilitating the data session. The message includes the information elements necessary to identify the PDP context.
10. The GGSN removes the PDP context from memory and returns a Delete PDP Context Response message to the SGSN. If the PDP context was the last associated with a particular dynamically assigned PDP Address, the GGSN will re-claim the IP address for use by subsequent PDP contexts.
11. The SGSN returns a Deactivate PDP Context Accept message to the MS.
12. The GGSN delivers the GGSN Charging Detail Records (G-CDRs) to a Charging Gateway (CG) using GTP Prime (GTPP). Note that, though not shown in this example, the GGSN could optionally be configured to send partial CDRs while the PDP context is active.
13. For each accounting message received from the GGSN, the CG responds with an acknowledgement.

## Mobile IP Call Flow

The following figure and the text that follows describe the call flow for a successful Corporate IP Connectivity data session.

```
sequenceDiagram
    participant MS
    participant GSM_BSS as GSM BSS/UMTS TRAN
    participant SGSN
    participant GGSN_FA as GGSN/FA
    participant CG
    participant AAA_Server as AAA Server
    participant HA
    participant Home_Network as Home Network

    MS->>GSM_BSS: 1
    Note over MS: 2
    MS->>SGSN: 3
    SGSN->>GGSN_FA: 4
    GGSN_FA->>AAA_Server: 5
    AAA_Server->>GGSN_FA: 6
    GGSN_FA->>SGSN: 7
    SGSN->>MS: 8
    Note over MS: 9
    MS->>GGSN_FA: 10
    MS->>GGSN_FA: 11
    GGSN_FA->>HA: 12
    HA->>GGSN_FA: 13
    GGSN_FA->>MS: 14
    SGSN->>MS: 15
    MS->>GGSN_FA: 16
    Note over MS, GGSN_FA, HA: DATA
    MS->>GGSN_FA: 17
    GGSN_FA->>HA: 18
    HA->>GGSN_FA: 19
    GGSN_FA->>MS: 20
    MS->>SGSN: 21
    SGSN->>GGSN_FA: 22
    GGSN_FA->>SGSN: 23
    SGSN->>MS: 24
    GGSN_FA->>CG: 25
    CG->>GGSN_FA: 26
```

Cisco ASR 5000 Series Gateway GPRS Support Node Administration Guide



2. The Terminal Equipment (TE) aspect of the MS sends AT commands to the Mobile Terminal (MT) aspect of the MS to place it into PPP mode.

The Link Control Protocol (LCP) is then used to configure the Maximum-Receive Unit size and the authentication protocol (Challenge-Handshake Authentication Protocol (CHAP), Password Authentication Protocol (PAP), or none). If CHAP or PAP is used, the TE will authenticate itself to the MT, which, in turn, stores the authentication information.

Upon successful authentication, the TE sends an Internet Protocol Control Protocol (IPCP) Configure-Request message to the MT. The message will either contain a static IP home address to use or request that one be dynamically assigned.

3. The MS sends an Activate PDP Context Request message that is received by an SGSN. The message contains information about the subscriber such as the Network layer Service Access Point Identifier (NSAPI), PDP Type, Access Point Name (APN), Quality of Service (QoS) requested, and PDP configuration options.

Note that regardless of whether or not the MS has a static address or is requesting a dynamic address, the “Requested PDP Address” field is omitted from the request when using Mobile IP.

4. The SGSN authenticates the request message and sends a Create PDP Context Request message to a GGSN using the GPRS Tunneling Protocol (GTPC, “C” indicates the control signaling aspect of the protocol). The recipient GGSN is selected based on either the request of the MS or is automatically selected by the SGSN. The message consists of various information elements including: PDP Type, Requested PDP con, APN, charging characteristics, and Tunnel Endpoint Identifier (TEID).

5. The GGSN determines if it can facilitate the session (in terms of memory or CPU resources, configuration, etc.) and creates a new entry in its PDP context list and provides a Charging ID for the session.

From the APN specified in the message, the GGSN determines how to handle the PDP context including whether or not Mobile IP should be used.

If authentication is required, the GGSN attempts to authenticate the subscriber locally against profiles stored in memory or send a RADIUS Access-Request message to an AAA server.

6. If the GGSN authenticated the subscriber to an AAA server, the AAA server responds with a RADIUS Access-Accept message indicating successful authentication.
7. The GGSN replies to the SGSN with a PDP Context Response using GTPC. The response will contain information elements such as the PDP Address, and PDP configuration options specified by the GGSN. Note that for Mobile IP, the GGSN returns a PDP Address of 0.0.0.0 indicating that it will be reset with a Home address after the PDP context activation procedure.
8. The SGSN returns an Activate PDP Context Accept message to the MS. The message includes response to the configuration parameters sent in the initial request.
9. The MT, will respond to the TE’s IPCP Config-request with an IPCP Config-Ack message. This ends the PPP mode between the MT and TE components of the MS.

Data can now be transmitted between the MS and the GGSN.

10. The FA component of the GGSN sends an Agent Advertisement message to the MS. The message contains the FA parameters needed by the mobile such as one or more care-of addresses. The message is sent as an IP limited broadcast message (i.e. destination address 255.255.255.255), however only on the requesting MS’s TEID to avoid broadcast over the radio interface.

11. The MS sends a Mobile IP Registration request to the GGSN/FA. This message includes either the MS’s static home address or it can request a temporary address by sending 0.0.0.0 as its home address. Additionally, the request must always include the Network Access Identifier (NAI) in a Mobile-Node-NAI Extension.

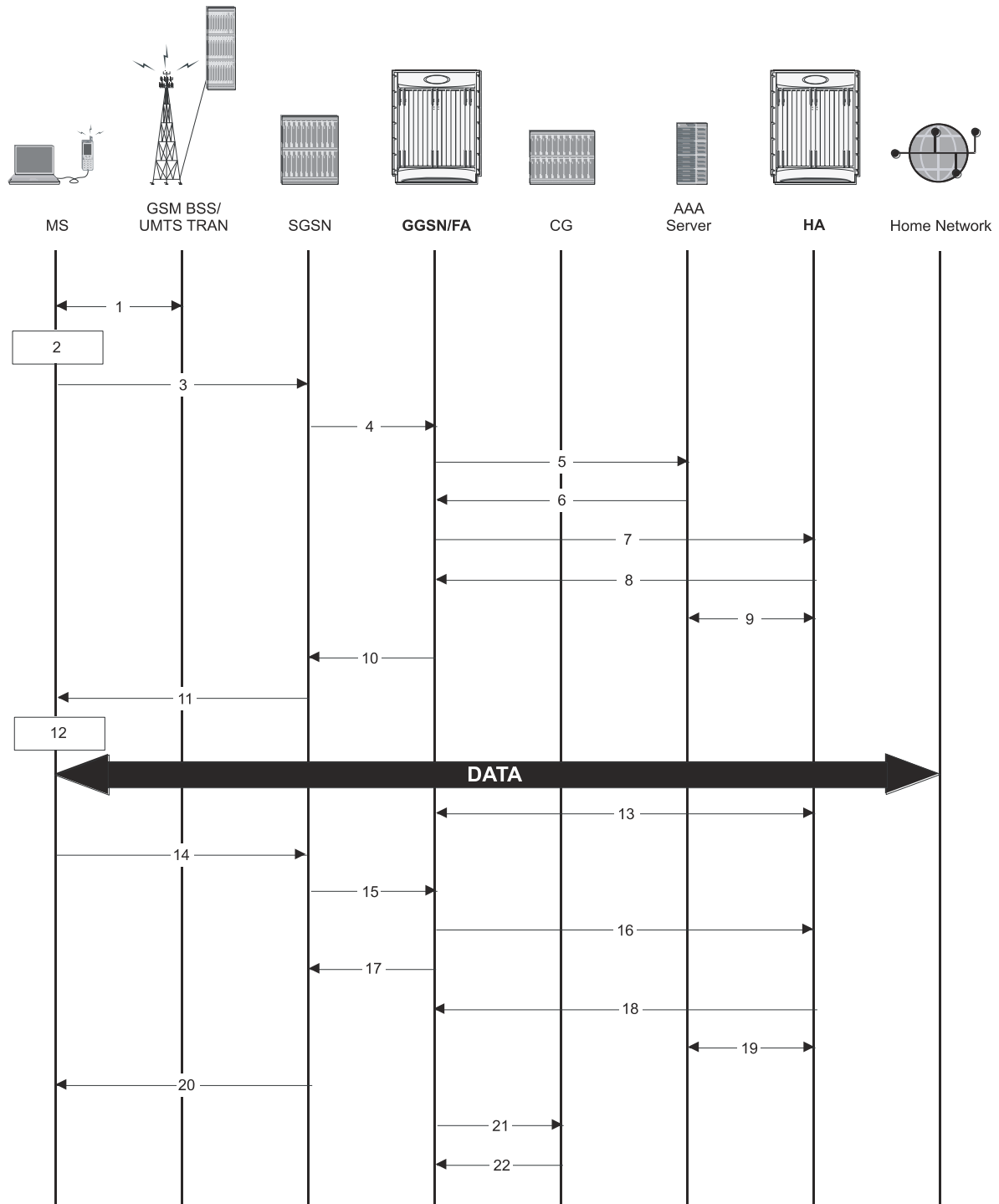
12. The FA forwards the registration request from the MS to the HA while the MS’s home address or NAI and TEID are stored by the GGSN.

13. The HA sends a registration response to the FA containing the address assigned to the MS.
14. The FA extracts the home address assigned to the MS by the HA from the response and the GGSN updates the associated PDP context. The FA then forwards it to the MS (identified by either the home address or the NAI and TEID).
15. The GGSN issues a PDP context modification procedure to the SGSN in order to update the PDP address for the MS.
16. The SGSN forwards the PDP context modification message to the MS.  
The MS can now send and receive data to or from their home network until the session is closed or times out. Note that for Mobile IP, only one PDP context is supported for the MS.
17. The MS can terminate the Mobile IP data session at any time. To terminate the Mobile IP session, the MS sends a Registration Request message to the GGSN/FA with a requested lifetime of 0.
18. The FA component forwards the request to the HA.
19. The HA sends a Registration Reply to the FA accepting the request.
20. The GGSN/FA forwards the response to the MN.
21. The MS sends a Deactivate PDP Context Request message that is received by the SGSN.
22. The SGSN sends a Delete PDP Context Request message to the GGSN facilitating the data session. The message includes the information elements necessary to identify the PDP context.
23. The GGSN removes the PDP context from memory and returns a Delete PDP Context Response message to the SGSN.
24. The SGSN returns a Deactivate PDP Context Accept message to the MS.
25. The GGSN delivers the GGSN Charging Detail Records (G-CDRs) to a Charging Gateway (CG) using GTP Prime (GTPP). Note that, though not shown in this example, the GGSN could optionally be configured to send partial CDRs while the PDP context is active.
26. For each accounting message received from the GGSN, the CG responds with an acknowledgement.

## Proxy Mobile IP Call Flows

The following figure and the text that follows describe a sample successful Proxy Mobile IP session setup call flow in which the MS receives its IP address from the HA.

Figure 18. HA Assigned IP Address Proxy Mobile IP Call Flow



1. The Mobile Station (MS) goes through the process of attaching itself to the GPRS/UMTS network.
2. The Terminal Equipment (TE) aspect of the MS sends AT commands to the Mobile Terminal (MT) aspect of the MS to place it into PPP mode.

The Link Control Protocol (LCP) is then used to configure the Maximum-Receive Unit size and the authentication protocol (Challenge-Handshake Authentication Protocol (CHAP), Password Authentication Protocol (PAP), or none). If CHAP or PAP is used, the TE will authenticate itself to the MT, which, in turn, stores the authentication information.

Upon successful authentication, the TE sends an Internet Protocol Control Protocol (IPCP) Configure-Request message to the MT. The message will either contain a static IP address to use or request that one be dynamically assigned.

3. The MS sends an Activate PDP Context Request message that is received by an SGSN. The message contains information about the subscriber such as the Network layer Service Access Point Identifier (NSAPI), PDP Type, PDP Address, Access Point Name (APN), Quality of Service (QoS) requested, and PDP configuration options.
4. The SGSN authenticates the request message and sends a Create PDP Context Request message to a GGSN using the GPRS Tunneling Protocol (GTPC, “C” indicates the control signaling aspect of the protocol). The recipient GGSN is selected based on either the request of the MS or is automatically selected by the SGSN. The message consists of various information elements including: PDP Type, PDP Address, APN, charging characteristics, and Tunnel Endpoint Identifier (TEID, if the PDP Address was static).
5. The GGSN determines if it can facilitate the session (in terms of memory or CPU resources, configuration, etc.) and creates a new entry in its PDP context list and provides a Charging ID for the session.  
  
From the APN specified in the message, the GGSN determines whether or not the subscriber is to be authenticated, if Proxy Mobile IP is to be supported for the subscriber, and if so, the IP address of the HA to contact.  
  
Note that Proxy Mobile IP support can also be determined by attributes in the user’s profile. Attributes in the user’s profile supersede APN settings.  
  
If authentication is required, the GGSN attempts to authenticate the subscriber locally against profiles stored in memory or send a RADIUS Access-Request message to an AAA server.
6. If the GGSN authenticated the subscriber to an AAA server, the AAA server responds with a RADIUS Access-Accept message indicating successful authentication and any attributes for handling the subscriber PDP context.
7. If Proxy Mobile IP support was either enabled in the APN or in the subscriber’s profile, the GGSN/FA forwards a Proxy Mobile IP Registration Request message to the specified HA. The message includes such things as the MS’s home address, the IP address of the FA (the care-of-address), and the FA-HA extension (Security Parameter Index (SPI)).
8. The HA responds with a Proxy Mobile IP Registration Response. The response includes an IP address from one of its locally configured pools to assign to the MS (its Home Address). The HA also creates a Mobile Binding Record (MBR) for the subscriber session.
9. The HA sends a RADIUS Accounting Start request to the AAA server which the AAA server responds to.
10. The GGSN replies with an affirmative Create PDP Context Response using GTPC. The response will contain information elements such as the PDP Address representing either the static address requested by the MS or the address assigned by the GGSN, the TEID used to reference PDP Address, and PDP configuration options specified by the GGSN.
11. The SGSN returns an Activate PDP Context Accept message to the MS. The message includes response to the configuration parameters sent in the initial request.
12. The MT, will respond to the TE’s IPCP Config-request with an IPCP Config-Ack message.

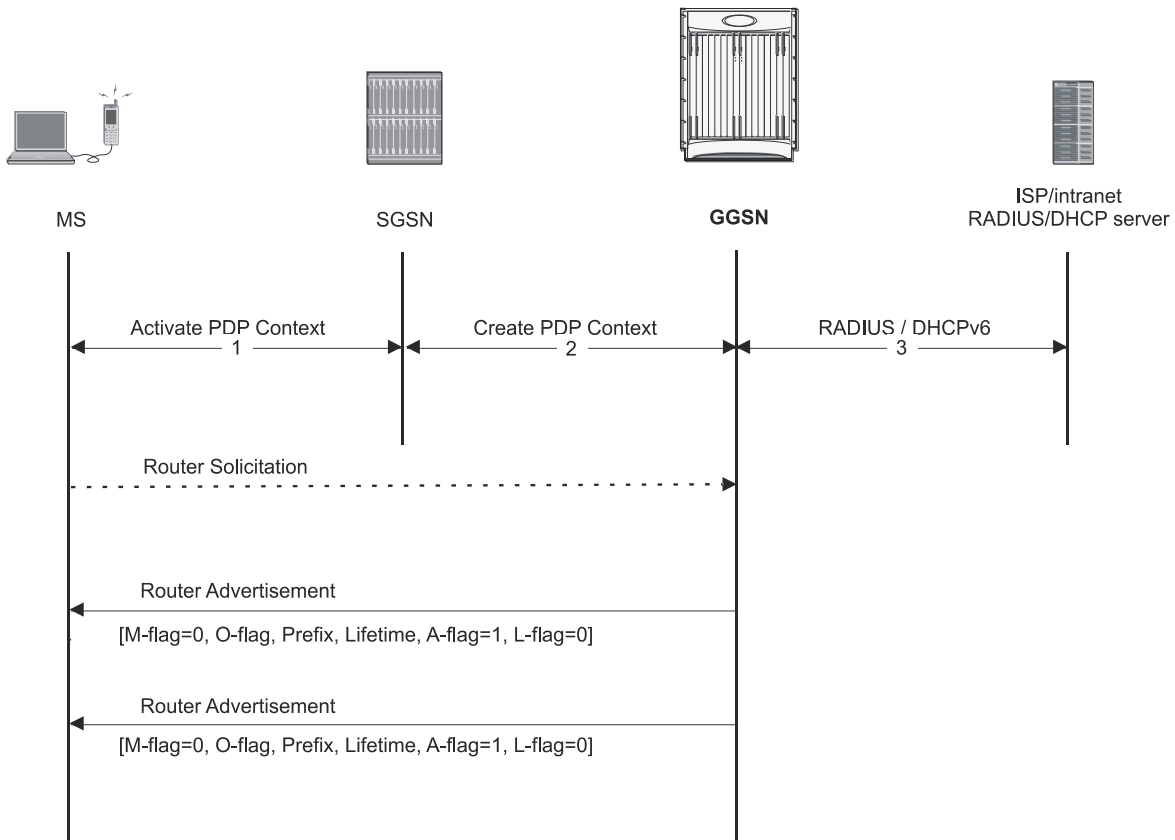
The MS can now send and receive data to or from the PDN until the session is closed or times out. Note that for Mobile IP, only one PDP context is supported for the MS.

13. The FA periodically sends Proxy Mobile IP Registration Request Renewal messages to the HA. The HA sends responses for each request.
14. The MS can terminate the data session at any time. To terminate the session, the MS sends a Deactivate PDP Context Request message that is received by the SGSN.
15. The SGSN sends a Delete PDP Context Request message to the GGSN facilitating the data session. The message includes the information elements necessary to identify the PDP context (i.e., TEID, and NSAPI).
16. The GGSN removes the PDP context from memory and the FA sends a Proxy Mobile IP Deregistration Request message to the HA.
17. The GGSN returns a Delete PDP Context Response message to the SGSN.
18. The HA replies to the FA with a Proxy Mobile IP Deregistration Request Response.
19. The HA sends a RADIUS Accounting Stop request to the AAA server which the AAA server responds to.
20. The SGSN returns a Deactivate PDP Context Accept message to the MS.
21. The GGSN delivers the GGSN Charging Detail Records (G-CDRs) to a Charging Gateway (CG) using GTP Prime (GTPP). Note that, though not shown in this example, the GGSN could optionally be configured to send partial CDRs while the PDP context is active.
22. For each accounting message received from the GGSN, the CG responds with an acknowledgement.

## IPv6 Stateless Address Auto Configuration Flows

The following figure and the text that follows describe a sample IPv6 stateless address auto configuration session setup call flow in which the MS receives its IP address from the RADIUS DHCP server.

Figure 19. IPv6 Stateless Address Auto Configuration Flow



1. The MS uses the IPv6 interface identifier provided by the GGSN to create its IPv6 link-local unicast address. Before the MS communicates with other hosts or mobile stations on the intranet/ISP, the MS must obtain an IPv6 global or site-local unicast address.
2. After the GGSN sends a create PDP context response message to the SGSN, it starts sending router advertisements periodically on the new MS-GGSN link established by the PDP context.
3. When creating a global or site-local unicast address, the MS may use the interface identifier received during the PDP context activation or it generates a new interface identifier. There is no restriction on the value of the interface identifier of the global or site-local unicast address, since the prefix is unique.

# Supported Standards

The GGSN complies with the following standards for 3GPP wireless data services.

- [3GPP References](#)
- [IETF References](#)
- [Object Management Group \(OMG\) Standards](#)

## 3GPP References

- 3GPP TS 09.60 v7.10.0 (2001-09): 3rd Generation Partnership project; Technical Specification Group Core Network; General Packet Radio Services (GPRS); GPRS Tunneling Protocol (GTP) across the Gn and Gp Interface (Release 1998) for backward compatibility with GTPv0
- 3GPP TS 23.060 v7.6.0 (2007-9): 3rd Generation Partnership project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS); Service description (Release 1999) as an additional reference for GPRS/UMTS procedures
- 3GPP TS 23.107 v7.1.0 (2007-09): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; QoS Concept and Architecture
- 3GPP TS 23.203 V7.7.0 (2006-08): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Policy and charging control architecture (Release 7)
- 3GPP TS 23.246 v7.4.0 (2007-09): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Multimedia Broadcast/Multicast Service (MBMS); Architecture and functional description (Release 7)
- 3GPP TS 24.008 v7.11.0 (2001-06): Mobile radio interface layer 3 specification; Core Network Protocols- Stage 3 (Release 1999) as an additional reference for GPRS/UMTS procedures
- 3GPP TS 29.060 v7.9.0 (2008-09): 3rd Generation Partnership Project; Technical Specification Group Core Network; General Packet Radio Services (GPRS); GPRS Tunneling Protocol (GTP) across the Gn and Gp Interface (Release 4) for the Core GTP Functionality
- 3GPP TS 29.061 v7.7.0 (2008-09): 3rd Generation Partnership Project; Technical Specification Group Core Network; Packet Domain; Interworking between the Public Land Mobile Network (PLMN) supporting Packet Based Services and Packet Data Networks (PDN)
- 3GPP TS 29.212 v7.6.0 (2008-09) 3rd Generation Partnership Project, Technical Specification Group Core Network and Terminals; Policy and Charging Control over Gx reference point (Release 7)
- 3GPP TS 29.213 V7.5.0 (2005-08): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control signalling flows and QoS parameter mapping; (Release 7)
- 3GPP TR 29.846 6.0.0 (2004-09) 3rd Generation Partnership Project, Technical Specification Group Core Networks; Multimedia Broadcast/Multicast Service (MBMS); CN1 procedure description (Release 6)
- 3GPP TS 32.015 v3.12.0 (2003-12): 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects; Telecommunication Management; Charging management; Call and event data for the Packet Switched (PS) domain (Release 1999) for support of Charging on GGSN

- 3GPP TS 32.215 v5.9.0 (2005-06): 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects; Telecommunication Management; Charging Management; Charging data description for the Packet Switched (PS) domain (Release 5)
- 3GPP TS 32.251 v7.5.1 (2007-10): 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects; Telecommunication management; Charging management; Packet Switched (PS) domain charging (Release 7)
- 3GPP TS 32.298 v7.4.0 (2007-09): 3rd Generation Partnership Project; Technical Specification Group Service and System Aspects; Telecommunication management; Charging management; Charging Data Record (CDR) parameter description
- 3GPP TS 32.299 v7.7.0 (2007-10): 3rd Generation Partnership Project; Technical Specification Group Service and System Aspects; Telecommunication management; Charging management; Diameter charging applications (Release 7)
- 3GPP TS 32.403 V7.1.0: Technical Specification Performance measurements - UMTS and combined UMTS/GSM
- 3GPP TS 33.106 V7.0.1 (2001-06): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Lawful Interception requirements (Release 7)
- 3GPP TS 33.107 V7.7.0 (2007-09): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Lawful interception architecture and functions (Release 7)

## IETF References

- RFC-768, User Datagram Protocol (UDP), August 1980
- RFC-791, Internet Protocol (IP), September 1982
- RFC-793, Transmission Control Protocol (TCP), September 1981
- RFC-894, A Standard for the Transmission of IP Datagrams over Ethernet Networks, April 1984
- RFC-1089, SNMP over Ethernet, February 1989
- RFC-1144, Compressing TCP/IP headers for low-speed serial links, February 1990
- RFC-1155, Structure & identification of management information for TCP/IP-based Internets, May 1990
- RFC-1157, Simple Network Management Protocol (SNMP) Version 1, May 1990
- RFC-1212, Concise MIB Definitions, March 1991
- RFC-1213, Management Information Base for Network Management of TCP/IP-based Internets: MIB-II, March 1991
- RFC-1215, A Convention for Defining Traps for use with the SNMP, March 1991
- RFC-1224, Techniques for managing asynchronously generated alerts, May 1991
- RFC-1256, ICMP Router Discovery Messages, September 1991
- RFC-1305, Network Time Protocol (Version 3) Specification, Implementation and Analysis, March 1992
- RFC-1332, The PPP Internet Protocol Control Protocol (IPCP), May 1992
- RFC-1398, Definitions of Managed Objects for the Ethernet-Like Interface Types, January 1993
- RFC-1418, SNMP over OSI, March 1993
- RFC-1570, PPP LCP Extensions, January 1994
- RFC-1643, Definitions of Managed Objects for the Ethernet-like Interface Types, July 1994



- RFC-1661, The Point to Point Protocol (PPP), July 1994
- RFC-1662, PPP in HDLC-like Framing, July 1994
- RFC-1701, Generic Routing Encapsulation (GRE), October 1994
- RFC-1850, OSPF Version 2 Management Information Base, November 1995
- RFC-1901, Introduction to Community-based SNMPv2, January 1996
- RFC-1902, Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2), January 1996
- RFC-1903, Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2), January 1996
- RFC-1904, Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2), January 1996
- RFC-1905, Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2), January 1996
- RFC-1906, Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2), January 1996
- RFC-1907, Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2), January 1996
- RFC-1908, Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework, January 1996
- RFC-1918, Address Allocation for Private Internets, February 1996
- RFC-1919, Classical versus Transparent IP Proxies, March 1996
- RFC-1962, The PPP Compression Control Protocol (CCP), June 1996
- RFC-1974, PPP STAC LZS Compression Protocol, August 1996
- RFC-2002, IP Mobility Support, May 1995
- RFC-2003, IP Encapsulation within IP, October 1996
- RFC-2004, Minimal Encapsulation within IP, October 1996
- RFC-2005, Applicability Statement for IP Mobility Support, October 1996
- RFC-2118, Microsoft Point-to-Point Compression (MPPC) Protocol, March 1997
- RFC 2131, Dynamic Host Configuration Protocol
- RFC 2132, DHCP Options and BOOTP Vendor Extensions
- RFC-2136, Dynamic Updates in the Domain Name System (DNS UPDATE)
- RFC-2211, Specification of the Controlled-Load Network Element Service
- RFC-2246, The Transport Layer Security (TLS) Protocol Version 1.0, January 1999
- RFC-2290, Mobile-IPv4 Configuration Option for PPP IPCP, February 1998
- RFC-2328, OSPF Version 2, April 1998
- RFC-2344, Reverse Tunneling for Mobile IP, May 1998
- RFC-2394, IP Payload Compression Using DEFLATE, December 1998
- RFC 2401, Security Architecture for the Internet Protocol
- RFC 2402, IP Authentication Header (AH)

- RFC 2406, IP Encapsulating Security Payload (ESP)
- RFC 2409, The Internet Key Exchange (IKE)
- RFC-2460, Internet Protocol Version 6 (IPv6)
- RFC-2461, Neighbor Discovery for IPv6
- RFC-2462, IPv6 Stateless Address Autoconfiguration
- RFC-2474, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers, December 1998
- RFC-2475, An Architecture for Differentiated Services, December 1998
- RFC-2484, PPP LCP Internationalization Configuration Option, January 1999
- RFC-2486, The Network Access Identifier (NAI), January 1999
- RFC-2571, An Architecture for Describing SNMP Management Frameworks, April 1999
- RFC-2572, Message Processing and Dispatching for the Simple Network Management Protocol (SNMP), April 1999
- RFC-2573, SNMP Applications, April 1999
- RFC-2574, User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3), April 1999
- RFC-2597, Assured Forwarding PHB Group, June 1999
- RFC-2598, Expedited Forwarding PHB, June 1999
- RFC-2618, RADIUS Authentication Client MIB, June 1999
- RFC-2620, RADIUS Accounting Client MIB, June 1999
- RFC-2661, Layer Two Tunneling Protocol “L2TP”, August 1999
- RFC-2697, A Single Rate Three Color Marker, September 1999
- RFC-2698, A Two Rate Three Color Marker, September 1999
- RFC-2784, Generic Routing Encapsulation (GRE) - March 2000, IETF
- RFC-2794, Mobile IP Network Access Identifier Extension for IPv4, March 2000
- RFC-2809, Implementation of L2TP Compulsory Tunneling via RADIUS, April 2000
- RFC-2845, Secret Key Transaction Authentication for DNS (TSIG), May 2000
- RFC-2865, Remote Authentication Dial In User Service (RADIUS), June 2000
- RFC-2866, RADIUS Accounting, June 2000
- RFC-2867, RADIUS Accounting Modifications for Tunnel Protocol Support, June 2000
- RFC-2868, RADIUS Attributes for Tunnel Protocol Support, June 2000
- RFC-2869, RADIUS Extensions, June 2000
- RFC-3007, Secure Domain Name System (DNS) Dynamic Update, November 2000
- RFC-3012, Mobile IPv4 Challenge/Response Extensions, November 2000
- RFC-3056, Connection of IPv6 Domains via IPv4 Clouds, February 2001
- RFC-3101 OSPF-NSSA Option, January 2003
- RFC-3143, Known HTTP Proxy/Caching Problems, June 2001
- RFC-3193, Securing L2TP using IPSEC, November 2001

- RFC-3314, Recommendations for IPv6 in Third Generation Partnership Project (3GPP) Standards, September 2002
- RFC-3316, Internet Protocol Version 6 (IPv6) for Some Second and Third Generation Cellular Hosts, April 2003
- RFC-3706, A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers, February 2004
- RFC-3543, Registration Revocation in Mobile IPv4, August 2003
- RFC 3588, Diameter Base Protocol, September 2003
- RFC 4006, Diameter Credit-Control Application, August 2005
- Draft, Route Optimization in Mobile IP
- Draft, Generalized Key Distribution Extensions for Mobile IP
- Draft, AAA Keys for Mobile IP

## Object Management Group (OMG) Standards

CORBA 2.6 Specification 01-09-35, Object Management Group



# Chapter 2

## Understanding the Service Operation

---

The system provides wireless carriers with a flexible solution for providing Gateway GPRS Support Node (GGSN) functionality for GPRS or UMTS networks.

The system functioning as a GGSN is capable of supporting the following types of subscriber data sessions:

- **Transparent IP:** The subscriber is provided basic access to a packet data network (PDN) without the GGSN authenticating the subscriber. Either a static or dynamic IP address can be assigned to the MS in this scenario.
- **Non-transparent IP:** The GGSN provides subscriber authentication services for the data session. Either a static or dynamic IP address can be assigned to the MS in this scenario.
- **Network-initiated:** An IP Packet Data Unit (PDP) is received by the GGSN from the PDN for a specific subscriber. If configured to support network-initiated sessions, the GGSN, will initiate the process of paging the MS and establishing a PDP context.
- **PPP Direct Access:** The GGSN terminates the subscribers PPP session and provides subscriber authentication services for the data session. Either a static or dynamic IP address can be assigned to the MS in this scenario.
- **Virtual Dialup Access:** The GGSN functions as an LAC, encapsulates subscriber packets using L2TP, and tunnels them directly to an LNS for processing.
- **Corporate IP VPN Connectivity:** Similar to the Virtual Dialup Access model, however, the GGSN is configured to tunnel subscriber packets to a corporate server using a protocol such as IP-in-IP.

Prior to connecting to the command line interface (CLI) and beginning the system's configuration, there are important things to understand about how the system supports these applications. This chapter provides terminology and background information that must be considered before attempting to configure the system.

# Terminology

This section defines some of the terms used in the chapters that follow.

## Contexts

A context is a logical grouping or mapping of configuration parameters that pertain to various physical ports, logical IP interfaces, and services. A context can be thought of as a virtual private network (VPN).

The system supports the configuration of multiple contexts. Each is configured and operates independently from the others. Once a context has been created, administrative users can then configure services, logical IP interfaces, subscribers, etc. for that context. Administrative users would then bind the logical interfaces to physical ports.

Contexts can also be assigned domain aliases, wherein if a subscriber's domain name matches one of the configured alias names for that context, then that context is used.

Contexts on the system can be categorized as follows:

- **Source context:** Also referred to as the “ingress” context, this context provides the subscriber's point-of-entry in the system. It is also the context in which services are configured. For example, in a GPRS/UMTS network, the radio network containing the Service GPRS Support Nodes (SGSNs) would communicate with the system via Gn interfaces configured within the source context as part of the GGSN service.
- **Destination context:** Also referred to as the “egress” context, this context is where a subscriber is provided services (such as access to the Internet) as defined by access point name (APN) configuration templates. For example, the system's destination context would be configured with the interfaces facilitating subscriber data traffic to/from the Internet, a VPN, or other PDN.
- **Authentication context:** This context provides authentication functionality for subscriber PDP contexts and/or administrative user sessions and contains the policies and logical interfaces for communicating with Remote Authentication Dial In User Service (RADIUS) authentication servers.

For subscriber authentication, this functionality must be configured in the same system context as the APN template(s). Optionally, to simplify the configuration process, both subscriber RADIUS authentication functionality and APN templates can be configured in the destination context.



**Important:** To ensure scalability, authentication functionality for subscriber sessions should not be configured in the local context.

For administrative users, authentication functionality can either be configured in the local context or be authenticated in the same context as subscribers.

- **Accounting context:** This context provides accounting functionality for subscriber PDP contexts and/or administrative user sessions.

The system context in which accounting functionality is configured depends on the protocol used. Accounting for subscriber PDP contexts can be performed using either the GPRS Tunneling Protocol Prime (GTPP) or RADIUS. Accounting for administrative user sessions is based on RADIUS.

When using GTPP, it is recommended that accounting functionality be configured in a system source context along with the GGSN service.

When using RADIUS for subscriber accounting, it must be configured in the same context as RADIUS authentication. To simplify the configuration process, RADIUS-based authentication and accounting can be configured in a destination context as long as the APN templates are configured there as well.

RADIUS-based accounting for administrative user sessions can either be configured in the local context or in the same context used for subscriber accounting.



**Important:** To ensure scalability, accounting functionality for subscriber sessions should not be configured in the local context.

- **Local context:** This is the default context on the system used to provide out-of-band management functionality. The local context is described in the Command Line Reference.

## Logical Interfaces

Prior to allowing the flow of user data, the port must be associated with a virtual circuit or tunnel called a logical interface. A logical interface within the system is defined as the logical assignment of a virtual router instance that provides higher-layer protocol transport, such as Layer 3 IP addressing. Interfaces are configured as part of the VPN context and are independent from the physical port that will be used to bridge the virtual interfaces to the network.

Logical interfaces are assigned to IP addresses and are bound to a specific port during the configuration process. Logical interfaces are also associated with services through bindings. Services are bound to an IP address that is configured for a particular logical interface. When associated, the interface takes on the characteristics of the functions enabled by the service. For example, if an interface is bound to a GGSN service, it will function as a Gn interface between the GGSN service and the SGSN. Services are defined later in this section.

There are several types of logical interfaces that must be configured to support the service as described below:

- **Gn:** This is the interface used by the GGSN to communicate with SGSNs on the same GPRS/UMTS Public Land Mobile Network (PLMN). This interface serves as both the signalling and data path for establishing and maintaining subscriber PDP contexts.

The GGSN communicates with SGSNs on the PLMN using the GPRS Tunnelling Protocol (GTP). The signalling or control aspect of this protocol is referred to as the GTP Control Plane (GTPC) while the encapsulated user data traffic is referred to as the GTP User Plane (GTPU).

One or more Gn interfaces can be configured per system context. Gn interfaces are bound to ports on either the Ethernet 10/100 or Ethernet 1000 Line Cards or on the four-port Quad Gig-E Line Card (QGLC).

- **Ga:** This is the interface used by the GGSN to communicate with the charging gateway (CG). The charging gateway is responsible for sending GGSN charging detail records (G-CDRs) received from the GGSN for each PDP context to the billing system.

The GGSN communicates with the CGs on the PLMN using GTP Prime (GTPP).

One or more Ga interfaces can be configured per system context. Ga interfaces are bound to ports on either the Ethernet 10/100 or Ethernet 1000 Line Cards or on the QGLC.

- **Gc:** This is the interface used by the GGSN to communicate with the Home Location Register (HLR) via a GTP-to-MAP (Mobile Application Part) protocol convertor. This interface is used for network initiated PDP contexts.

For network initiated PDP contexts, the GGSN will communicate with the protocol convertor using GTP. The convertor, in turn, will communicate with the HLR using MAP over Signalling System 7 (SS7).

One Gc interface can be configured per system context. Gc interfaces are bound to ports on either the Ethernet 10/100 or Ethernet 1000 Line Cards or on the QGLC.

- **Gi:** This is the interface used by the GGSN to communicate with packet data networks (PDNs) external to the PLMN. Examples of PDNs are the Internet or corporate intranets.  
Additionally, inbound packets received on this interface could initiate a network requested PDP context if the intended MS is not currently connected.  
One or more Gi interfaces can be configured per system context. Gi interfaces are bound to ports on either the Ethernet 10/100 or Ethernet 1000 Line Cards or on the QGLC.
- **Gp:** This is the interface used by the GGSN to communicate with GPRS support nodes (GSNs, e.g. GGSNs and/or SGSNs) on different PLMNs. Within the system, a single interface can serve as both a Gn and a Gp interface.  
One or more Gn/Gp interfaces can be configured per system context. Gp interfaces are bound to ports on either the Ethernet 10/100 or Ethernet 1000 Line Cards or on the QGLC.
- **AAA:** This is the interface used by the GGSN to communicate with either an authentication or accounting server on the network using the Remote Authentication Dial In User Service (RADIUS) protocol.  
This is an optional interface that can be by the GGSN for subscriber PDP context authentication or accounting. AAA interfaces are bound to ports on either the Ethernet 10/100 or Ethernet 1000 Line Cards or on the QGLC.
- **S6b:** This is an optional Diameter protocol-based interface over which the GGSN communicates with 3G AAA/HSS in LTE/SAE network for subscriber authorization.



**Important:** This interface is supported through license-enabled feature. For more information on this support, refer *Common Gateway Access Support* in guide.

- **DHCP:** This is the interface used by the GGSN to communicate with a Dynamic Host Control Protocol (DHCP) Server. The system can be configured to dynamically provide IP addresses for PDP contexts from the DHCP server.  
DHCP interfaces are bound to ports on either the Ethernet 10/100 or Ethernet 1000 Line Cards or on the QGLC.

## Bindings

A binding is an association between “elements” within the system. There are two types of bindings: static and dynamic. Static binding is accomplished through the configuration of the system. Static bindings are used to associate:

- A specific logical interface (configured within a particular context) to a physical port. Once the interface is bound to the physical port, traffic can flow through the context just as if it were any physically defined circuit. Static bindings support any encapsulation method over any interface and port type.
- A service to an IP address assigned to a logical interface within the same context. This allows the interface to take on the characteristics (i.e., support the protocols) required by the service. For example, a GGSN service bound to a logical interface will cause the logical interface to take on the characteristics of a Gn interface within a GPRS/UMTS network.

Dynamic binding associates a subscriber to a specific egress context based on the configuration of their profile or system parameters. This provides a higher degree of deployment flexibility as it allows a wireless carrier to support multiple services and facilitates seamless connections to multiple networks.



## Services

Services are configured within a context and enable certain functionality. The following services can be configured on the system:

- **GGSN services:** GGSN services are configured to support both mobile-initiated and network-requested PDP contexts. The GGSN service must be bound to a logical interface within the same context. Once bound, the interface takes on the characteristics of a Gn interface. Multiple services can be bound to the same logical interface. Therefore, a single physical port can facilitate multiple Gn interfaces.

- **FA services:** FA services are configured to support Mobile IP and define FA functionality on the system.

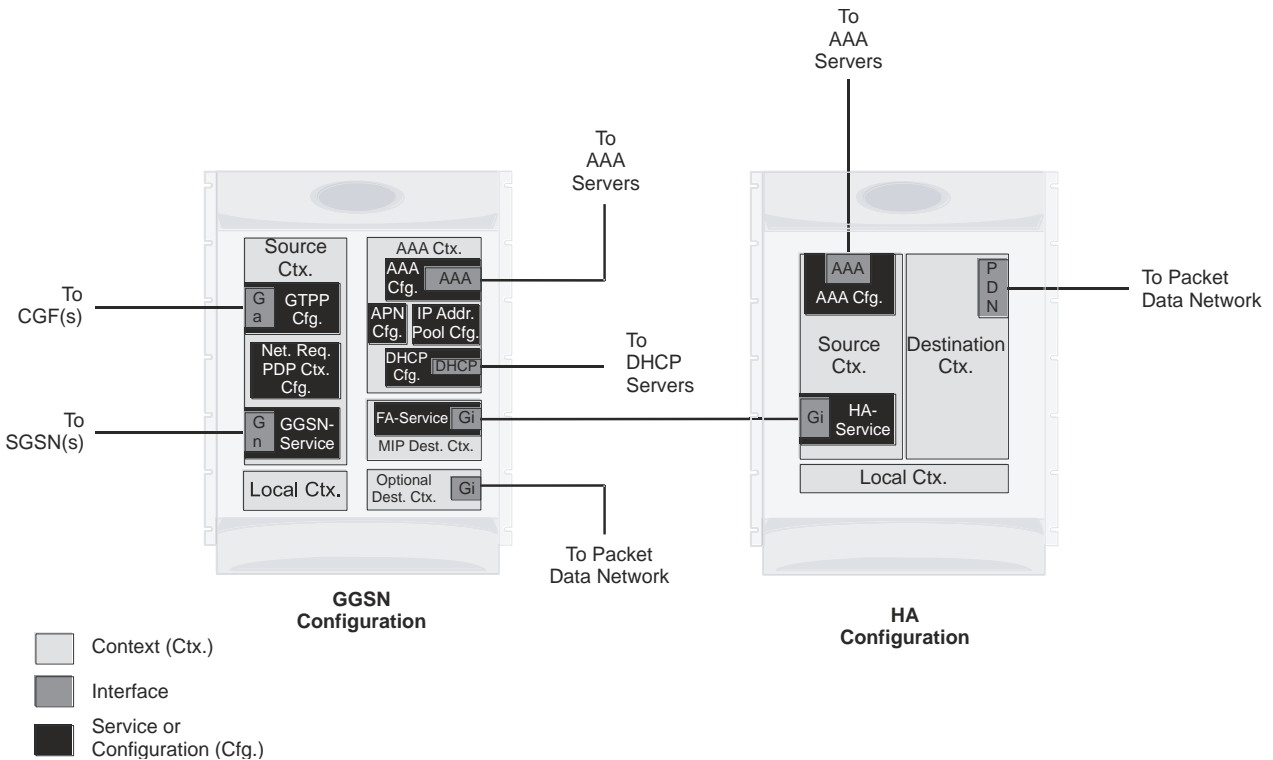
The system supports multiple Mobile IP configurations. A single system can perform the function of a FA only, an HA only, or a combined PDSN/FA/HA. Depending on your configuration, the FA service can create and maintain the Pi interface between the PDSN/FA and the HA or it can communicate with an HA service configured within the same context.

The FA service should be configured in a different context from the PDSN service. However, if the FA service will be communicating with an HA that is a separate network element, it must be configured within the same context as and be bound to the Pi interfaces that allow it to communicate with the HA.

- **LAC services:** LAC services are configured on the system to provide Layer 2 Tunneling Protocol (L2TP) access concentrator (LAC) functionality. LAC services can be configured and used within networks to provide secure tunneling to an L2TP network server (LNS) on a remote PDN.
- **DHCP services:** DHCP services are configured on a system to provide dynamic assignment of IP address to PDP contexts through the use of the Dynamic Host Configuration Protocol (DHCP).

Following figure illustrates the relationship between services, interfaces, and contexts within the system for GPRS/UMTS networks.

Figure 20. Service, Interface, and Context Relationship Within the System for GPRS/UMTS Networks



The source context used to service a subscriber session is the same as the context in which the GGSN service is configured. Each GGSN service is bound to an IP address in a source context. The SGSNs select which IP address to use, typically by using DNS. Once a subscriber has established a PDP context with a GGSN, the SGSNs continue to use that same PDP context and GGSN as the subscriber moves about the network.

Destination contexts are selected based on APN configuration. When the system receives a **Create PDP Context Request** message from the SGSN, it examines the APN that was provided. If the APN is not found on the system, the system rejects the request.

After the APN has been found, the system may choose a different APN based on the system's virtual APN configuration. In any event, a final APN is selected by the system.

The system determines the destination context to use based on a parameter contained within the final APN configuration. If a valid destination context name is configured for this parameter, it is used. If the name is not valid, or if it is not configured, the system uses the context in which the APN is configured.

Once the system locates the context in which the APN is configured, it uses that context for subscriber authentication and RADIUS-based accounting (if enabled). Any parameters returned by the RADIUS server during the subscriber authentication/authorization override APN configuration parameters.

If GTPP-based accounting is enabled, the system uses the source context for accounting. That context may be overridden by configuring a different accounting context to use in the GGSN service configuration.

## How the System Selects Contexts

This section provides details about the process that is used to determine which context to use for context-level administrative user and/or subscriber sessions. Understanding this process allows you to better plan your configuration in terms of how many contexts and interfaces need to be configured.

### Context Selection for Subscriber Sessions

The context selection process for a subscriber session is more involved than that for the administrative users.

The source context used to service a subscriber session is the same as the context in which the GGSN service is configured. Each GGSN service is bound to an IP address in a source context. The SGSNs select which IP address to use, typically by using DNS. Once a subscriber has established a PDP context with a GGSN, the SGSNs continue to use that same PDP context and GGSN as the subscriber moves about the network.

Destination contexts are selected based on APN configuration. When the system receives a **Create PDP Context Request** message from the SGSN, it examines the APN that was provided. If the APN is not found on the system, the system rejects the request.

After the APN has been found, the system may choose a different APN based on the system's virtual APN configuration. In any event, a final APN is selected by the system.

The system determines the destination context to use based on a parameter contained within the final APN configuration. If a valid destination context name is configured for this parameter, it is used. If the name is not valid, or if it is not configured, the system uses the context in which the APN is configured.

Once the system locates the context in which the APN is configured, it uses that context for subscriber authentication and RADIUS-based accounting (if enabled). Any parameters returned by the RADIUS server during the subscriber authentication/authorization override APN configuration parameters.

If GTPP-based accounting is enabled, the system uses the source context for accounting. That context may be overridden by configuring a different accounting context to use in the GGSN service configuration.



# Chapter 3

## GGSN Configuration Example

---

This chapter provides information for configuring the system to function as a Gateway GPRS Support Node (GGSN) in General Packet Radio Service (GPRS) or Universal Mobile Telecommunications System (UMTS) wireless data networks.



**Important:** This chapter does not discuss the configuration of the local context. Information about the local context can be found in the *Command Line Interface Overview* chapter of the *System Administration Guide* and the *Command Line Interface Reference*.

---

The most simple configuration that can be implemented on the system to support GGSN functionality requires that two contexts (one source and one destination) be configured on the system as shown in the following figure.

The source context facilitates the following:

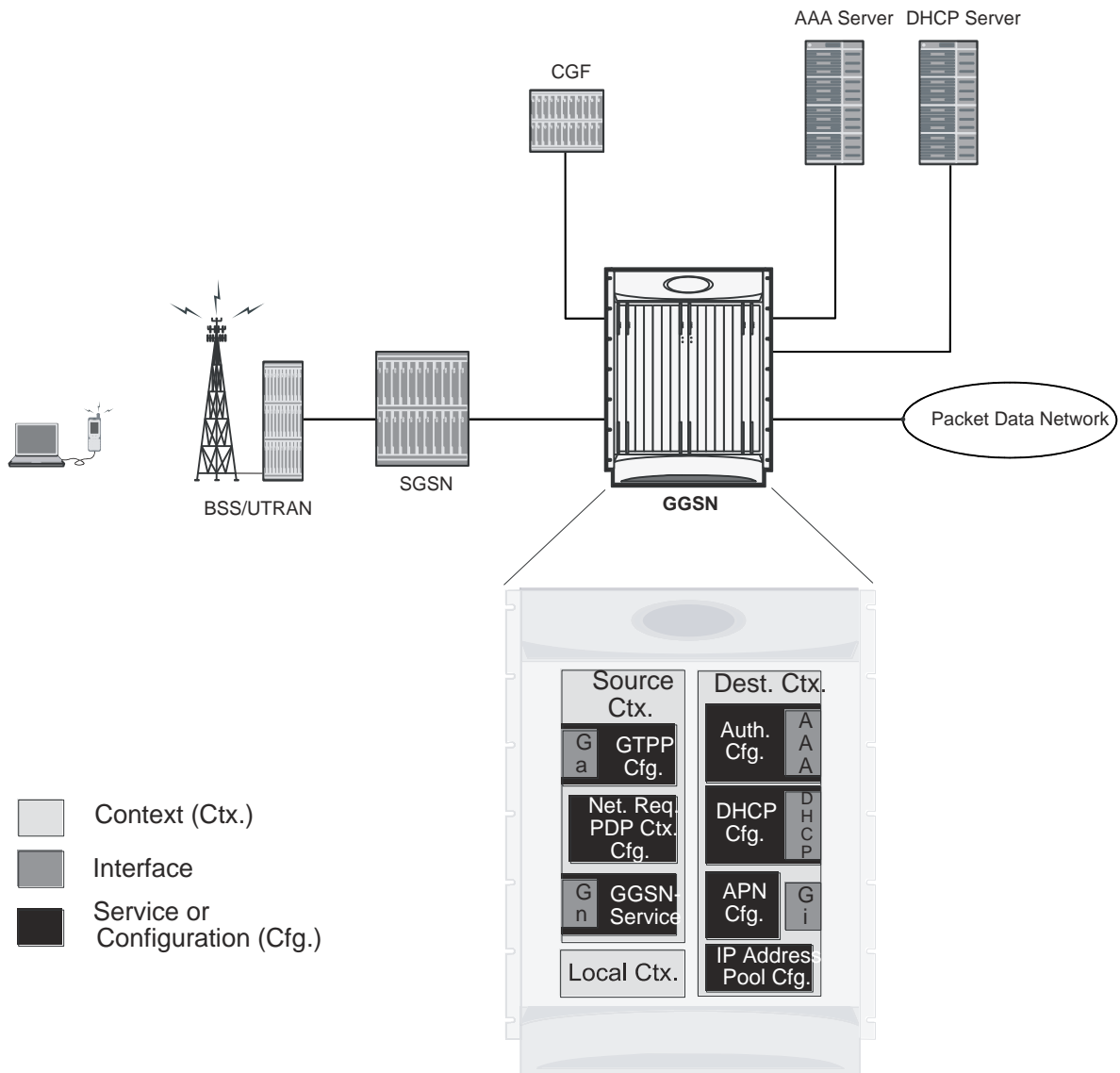
- GGSN service(s) and Gn interface to the Service GPRS Support Node (SGSN)
- GPRS Tunneling Protocol Prime (GTPP) configuration and Ga interface to the Charging Gateway Function (CGF)

The destination context facilitates the following:

- Access Point Name (APN) configuration
- RADIUS authentication configuration and the interface to the authentication server
- DHCP configuration and the interface to the DHCP server
- IP address pools
- Gi interface to the packet data network (PDN)

This configuration supports IP (transparent and non-transparent) and PPP PDP contexts as well as network requested PDP contexts.

Figure 21. GGSN Support Using a Single Source and Destination Context



# Information Required

The following sections describe the minimum amount of information required to configure and make the GGSN operational on the network. To make the process more efficient, it is recommended that this information be available prior to configuring the system.

There are additional configuration parameters that are not described in this section. These parameters deal mostly with fine-tuning the operation of the GGSN in the network. Information on these parameters can be found in the appropriate sections of the Command Line Reference.

## Source Context Configuration

The following table lists the information that is required to configure the source context.

**Table 1. Required Information for Source Context Configuration**

Required Information	Description
Source context name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the source context will be recognized by the system.
Gn Interface Configuration	
Gn interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	These will be assigned to the Gn interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	An identification string from 1 to 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the source context and are used to bind logical Gn interfaces.
Gateway IP address	Used when configuring static routes from the Gn interface(s) to a specific network.
GGSN service Configuration	
GGSN service name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the GGSN service will be recognized by the system. Multiple names are needed if multiple GGSN services will be used.
Accounting context	The name of the context configured on the system in which the processing of GTPP accounting records is performed. The context name is an identification string from 1 to 79 characters (alpha and/or numeric). By default, the system attempts to use the same context as the one in which the GGSN service is configured.

## ■ Information Required

Required Information	Description
UDP port number for GTPC traffic	The port used by the GGSN service and the SGSN for communicating GTPC sockets for GTPv1. The UDP port number and can be any integer value from 1 to 65535. The default value is 2123.
Public Land Mobile Network (PLMN) Identifiers	<b>Mobile Country Code (MCC):</b> The MCC can be configured to any integer value from 0 to 999.
	<b>Mobile Network Code (MNC):</b> The MNC can be configured to any integer value from 0 to 999.
SGSN information (optional)	The GGSN can be configured with information about the SGSN(s) that it is to communicate with. This includes the SGSN's IP address and subnet mask and whether or not the SGSN is on a foreign PLMN. Multiple SGSNs can be configured.
GGSN charging characteristics (CC) (optional)	<p><b>Behavior Bits:</b> If charging characteristics will be configured on the GGSN, behavior bits for the following conditions can be configured:</p> <ul style="list-style-type: none"> <li>• GGSN use of the accounting server specified by the profile index</li> <li>• GGSN rejection of Create PDP Context Request messages</li> <li>• GGSN ceases sending accounting records</li> </ul> <p>Each value must be a unique bit from 1 to 12 to represent the 12 possible behavior bits allowed for in the standards. The default configuration is disabled (0).</p>
	<p><b>Profile Index:</b> If the GGSN's charging characteristics will be used for subscriber PDP contexts, profile indexes can be modified/configured for one or more of the following conditions:</p> <ul style="list-style-type: none"> <li>• The number of statistics container changes is met or exceeded causing an accounting record to be closed. The number can be configured from 1 to 15. The default is 4.</li> <li>• The up and/or downlink traffic volume limits are met or exceeded within a specific time interval causing a partial record to be generated. The up and downlink volumes can be configured from 0 to 1000000 octets. The interval can be configured from 60 to 40000000 seconds.</li> <li>• The up and/or downlink traffic volume limits are met or exceeded causing an accounting record to be closed. The up and downlink volumes can be configured from 100000 to 4000000000 octets.</li> <li>• The number of SGSN switchovers is met or exceeded causing an accounting record to be closed. The number can be configured from 1 to 15. The default is 4.</li> <li>• Specific tariff times within a day are reached causing an accounting record to be closed. Up to four times can be configured using the hour of the day (1-24) and the minute (1-60).</li> <li>• Prepaid accounting can be disabled for a specified profile index.</li> </ul> <p>The system supports the configuration of up to 16 profile indexes numbered 0 through 15.</p>
PLMN policy	<p>The GGSN can be configured treat communications from unconfigured SGSNs in one of the following ways:</p> <ul style="list-style-type: none"> <li>• Treat the SGSN as if it is on a foreign PLMN</li> <li>• Treat the SGSN as if it is on a home PLMN</li> <li>• Reject communications from unconfigured SGSNs (default)</li> </ul>
Ga Interface Configuration	



Required Information	Description
Ga interface name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	These will be assigned to the Ga interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	An identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the source context and are used to bind logical Ga interfaces.
Gateway IP address	Used when configuring static routes from the Ga interface(s) to a specific network.
GTPP Configuration	
Charging gateway address	The IP address of the system's GGSN interface.
CGF server information	<b>IP address:</b> The IP address of the CGF server to which the GGSN will send accounting information. Multiple CGFs can be configured.
	<b>Priority:</b> If more than one CGF is configured, this is the server's priority. It is used to determine the rotation order of the CGFs when sending accounting information. The priority can be configured to any integer value from 1 to 1000. The default is 1.
	<b>Maximum number of messages:</b> The maximum number of outstanding or unacknowledged GTPP messages allowed for the CGF. The maximum number can be configured to any integer value from 1 to 256. The default is 256.
GCDR optional fields	The following optional fields can be specified/configured in CDRs generated by the GGSN: <ul style="list-style-type: none"> <li>diagnostics</li> <li>duration-ms (the time specified in the mandatory Duration field is reported in milliseconds)</li> <li>local-record-sequence-number</li> <li>plmn-id</li> </ul>
Network Requested PDP Context Support Configuration (optional)	
Activation Requirements	<b>IP address:</b> The static IP address of the mobile station's for which network-requested PDP context activation will be supported. Up to 1000 addresses can be configured.
	<b>Destination context name:</b> The name of the destination context configured on the system that contains the IP address pool containing the mobile station's static address.
	<b>International Mobile Subscriber Identity (IMSI):</b> The IMSI of the mobile station.
	<b>APN:</b> The name of the access point that will be passed to the SGSN by the GGSN for the mobile station.

Required Information	Description
GSN-map node	Communications with the HLR from the GGSN go through a GSN-map node that performs the protocol conversion from GTPC to SS7. The IP address of the map node must be configured. Only one GSN-map node can be configured per source context.

## Destination Context Configuration

The following table lists the information that is required to configure the destination context.

**Table 2. Required Information for Destination Context Configuration**

Required Information	Description
Destination context name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the destination context will be recognized by the system. <b>NOTE:</b> For this configuration, the destination context name should <b>not</b> match the domain name of a specific APN.
APN Configuration	
APN name	An identification string by which the APN will be recognized by the system. The name can be from 1 to 62 alpha and/or numeric characters and is not case sensitive. It may also contain dots ( . ) and/or dashes ( - ). Multiple names are needed if multiple APNs will be used.
Accounting mode	Selects the accounting protocol. GTPP or RADIUS are supported. In addition, accounting can be completely disabled. The default is to perform accounting using GTPP. <b>NOTE:</b> The examples discussed in this chapter assumes GTPP is used.
Authentication protocols used	Specifies how the system handles authentication: using a protocol (such as CHAP, PAP, or MSCHAP), or not requiring any authentication.
APN charging characteristics (CC) (optional)	Specifies whether or not the GGSN accepts the CC from the SGSN for home, visiting, and roaming subscribers. By default the GGSN accepts the CC from the SGSN for all three scenarios. If the GGSN is to use its own CC for any of these scenarios, then each scenario requires the specification of behavior bits and a profile index to use. <b>NOTE:</b> The profile index parameters are configured as part of the GGSN service.
Domain Name Service (DNS) information (optional)	If DNS will be used for the APN, IP addresses can be configured for primary and secondary DNS servers.

Required Information	Description
IP address allocation method	<p>Specifies how sessions facilitated by this APN will receive an IP address. IP addresses can be assigned using one of the following methods:</p> <ul style="list-style-type: none"> <li>• <b>Dynamic:</b> Address can be dynamically assigned from one of the sources. <ul style="list-style-type: none"> <li>• <b>Dynamic Host Control Protocol (DHCP) server:</b> The system can be configured to act as a DHCP proxy and receive address from the server in advance and assign them as needed or it can relay DHCP messages from the MS.</li> <li>• <b>Local address pools:</b> The system can be configured with local address pools.</li> </ul> </li> <li>• <b>Static:</b> MS IP addresses can be permanently assigned.</li> </ul> <p>By default, the system is configured to either dynamically assign addresses from a local pool and/or allow static addresses.</p>
IP address pool name	<p>If addresses will be dynamically assigned from a locally configured private pool, the name of the pool must be configured. If no name is configured, the system will automatically use any configured public pool.</p>
IP destination context name	<p>The name of the system destination context to use for subscribers accessing the APN. If no name is specified, the system automatically uses the system context in which the APN is configured.</p>
Maximum number of PDP contexts	<p>The maximum number of PDP contexts that are supported for the APN. The maximum number can be configured to any integer value from 1 to 1500000. The default is 1000000.</p>
PDP type	<p>The type of PDP contexts supported by the APN. The type can be IPv4, IPv6, both IPv4 and IPv6, or PPP. IPv4 support is enabled by default. For IPv6 PDP configuration, at least one IPv6 interface needs to be configured in the destination context.</p>
Verification selection mode	<p>The level of verification that will be used to ensure a MS's subscription to use the APN. The GGSN uses any of the following methods:</p> <ul style="list-style-type: none"> <li>• No verification and MS supplies APN</li> <li>• No verification and SGSN supplies APN</li> <li>• Verified by SGSN (default)</li> </ul>
DHCP Interface Configuration (optional)	
DHCP interface name	<p>An identification string from 1 to 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured.</p>
IP address and subnet	<p>These will be assigned to the DHCP interface and be bound to the DHCP service. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.</p>
Gateway IP address	<p>Used when configuring static routes from the DHCP interface(s) to a specific network.</p>
Physical port number	<p>The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.</p>

## ■ Information Required

Required Information	Description
Physical port description	An identification string from 1 to 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the source context and are used to bind logical DHCP interfaces.
DHCP Service Configuration (optional)	
DHCP Service Name	This is an identification string between 1 and 63 characters (alpha and/or numeric) by which the DHCP service will be recognized by the system. Multiple names are needed if multiple GGSN services will be used.
DHCP Server Information	The IP address of each DHCP server that the system is to communicate with must be configured. Multiple servers can be configured. If multiple servers are configured, each can be assigned a priority from 1 to 1000. The default priority is 1.
Lease Duration	Specifies the minimum and maximum allowable lease times that are accepted in responses from DHCP servers. <ul style="list-style-type: none"> <li>• <b>Minimum Lease Time:</b> Measured in seconds and can be configured to any integer value from 600 to 3600. The default is 600 seconds.</li> <li>• <b>Maximum Lease Time:</b> Measured in seconds and can be configured to any integer value from 10800 to 4294967295. The default is 86400 seconds.</li> </ul>
AAA Interface Configuration	
AAA interface name	This is an identification string from 1 to 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	These will be assigned to the AAA interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	This is an identification string from 1 to 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are used to bind logical AAA interfaces.
Gateway IP address	Used when configuring static routes from the AAA interface(s) to a specific network.
RADIUS Server Configuration	
RADIUS Authentication server	<b>IP Address:</b> Specifies the IP address of the RADIUS authentication server the system will communicate with to provide subscriber authentication functions. Multiple addresses are needed if multiple RADIUS servers will be configured. If multiple servers are configured, each can be assigned a priority.
	<b>Shared Secret:</b> The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the RADIUS authentication server and the source context. A shared secret is needed for each configured RADIUS server.

Required Information	Description
	<b>UDP Port Number:</b> Specifies the port used by the source context and the RADIUS authentication server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1812.
RADIUS Accounting server (optional)	<b>IP Address:</b> Specifies the IP address of the RADIUS accounting server that the source context will communicate with to provide subscriber accounting functions. Multiple addresses are needed if multiple RADIUS servers will be configured. RADIUS accounting servers are configured within the source context. Multiple servers can be configured and each assigned a priority.
	<b>Shared Secret:</b> The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the RADIUS accounting server and the source context. A shared secret is needed for each configured RADIUS server.
	<b>UDP Port Number:</b> Specifies the port used by the source context and the RADIUS Accounting server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1813.
RADIUS attribute NAS Identifier	Specifies the name by which the source context will be identified in the Access-Request message(s) it sends to the RADIUS server. The name must be from 1 to 32 alpha and/or numeric characters and is case sensitive.
RADIUS NAS IP address	Specifies the IP address of the system's AAA interface. A secondary address can be optionally configured.
PDN Interface Configuration	
PDN interface name	This is an identification string from 1 to 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. PDN interfaces are configured in the destination context.
IP address and subnet	These will be assigned to the PDN interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description(s)	This is an identification string from 1 to 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions will be needed if multiple ports will be used. Physical ports are configured within the destination context and are used to bind logical PDN interfaces.
Gateway IP address(es)	Used when configuring static routes from the PDN interface(s) to a specific network.
IP Address Pool Configuration	
IP address pool name(s)	This is an identification string from 1 to 31 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions will be needed if multiple ports will be used.

## ■ Information Required

Required Information	Description
Pool addresses, subnet mask and type	<p>The pool can consist of either of the following:</p> <ul style="list-style-type: none"><li>• An entire subnet configured using the initial address and the subnet mask</li><li>• A range of addresses configured using the first and last IP addresses in the range</li></ul> <p>The pool can be configured as public, private, or static. Public pools can also be assigned a priority.</p>

## How This Configuration Works

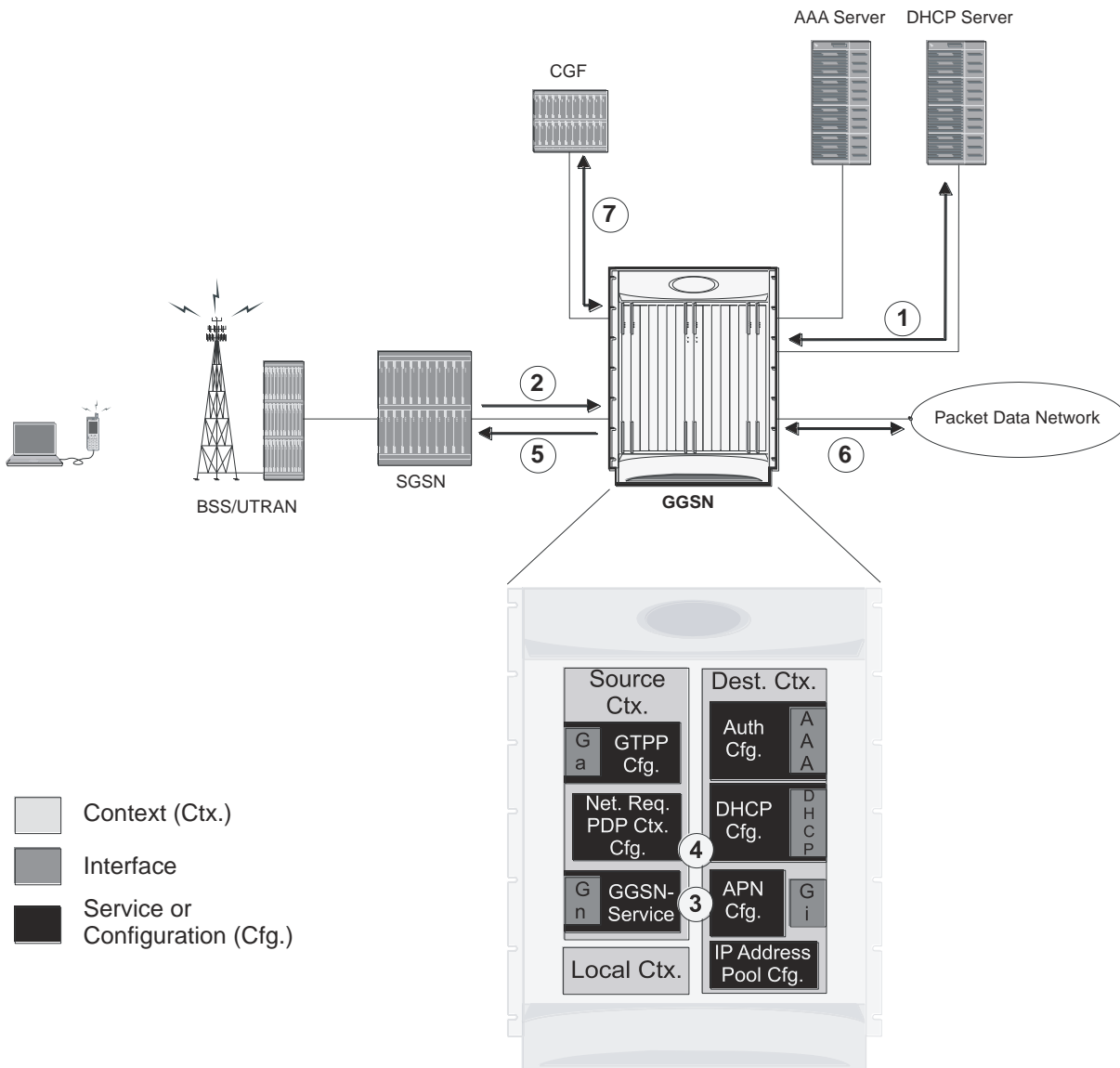
This section provides a description of how the information detailed in the previous sections of this chapter are used in the processing of the following types of subscriber sessions:

- [Transparent IP PDP Context Processing](#)
- [Non-transparent IP PDP Context Processing](#)
- [PPP PDP Context Processing](#)
- [Network-requested PDP Context Processing](#)

### Transparent IP PDP Context Processing

The following figure and the text that follows describe how this configuration with a single source and destination context would be used by the system to process a transparent IP PDP context.

Figure 22. Transparent IP PDP Context Call Processing



1. If the DHCP client mode is used for the dynamic assignment of IP addresses for subscriber PDP contexts, the system will retrieve addresses from the server over the DHCP interface during boot up and store them in cache memory.
2. A Create PDP Context Request message for a subscriber session is sent from the SGSN to the GGSN service over the Gn interface. The message contains information such as the PDP Type, APN, and charging characteristics.
3. The GGSN determines whether or not it is configured with an APN identical to the one specified in the message. If so, it determines how to process the session based on the configuration of the APN.
4. If the MS requires a dynamically assigned address, the GGSN assigns one from those stored in its memory cache.
5. The GGSN returns an affirmative Create PDP Context Response to the SGSN over the Gn interface.

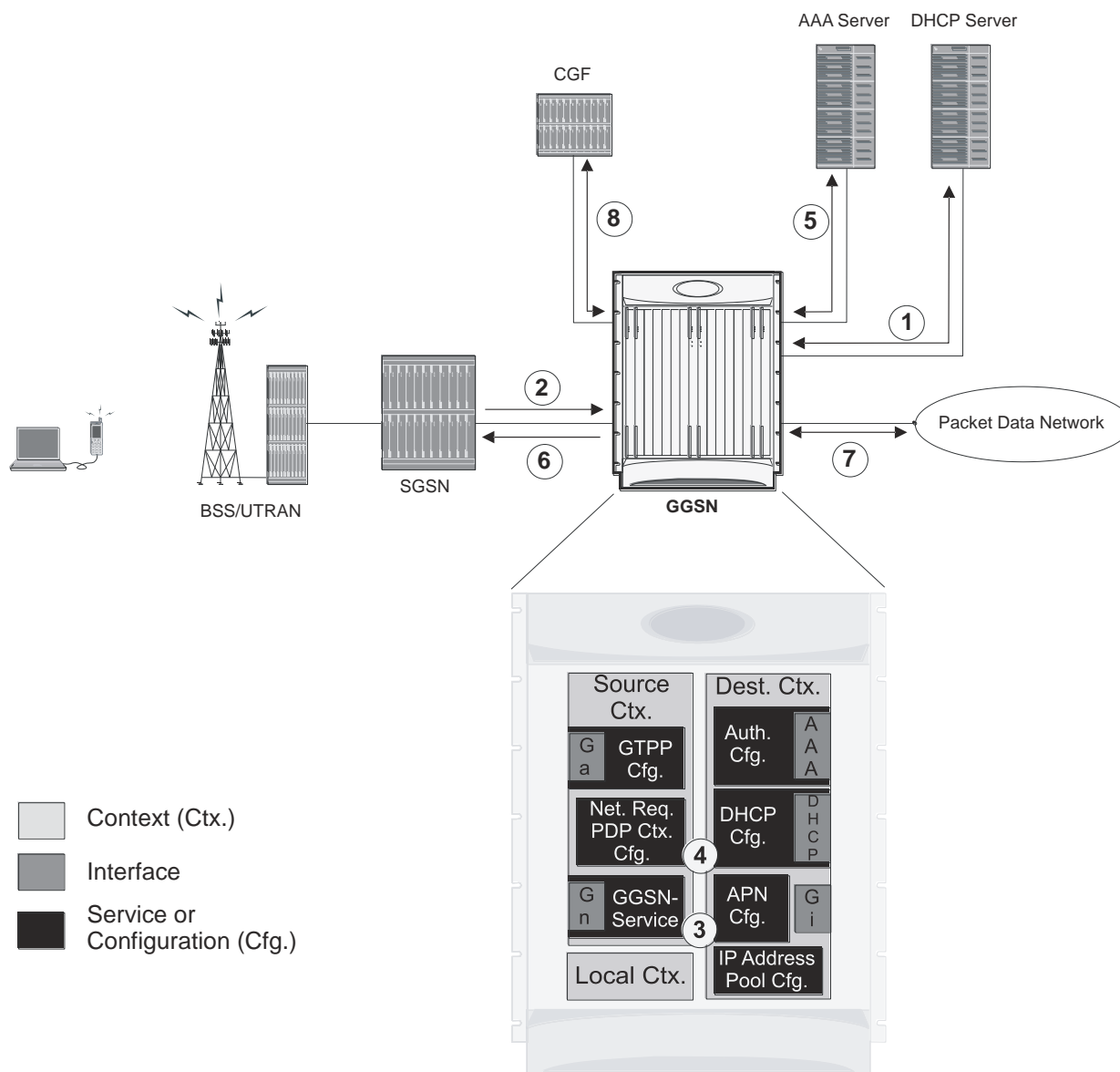


6. The MS sends/receives data to/from the packet data network over the GGSN's PDN interface.
7. Upon termination of the subscriber session, the GGSN sends GGSN charging detail records to the CGF using GTPP over the Ga interface.

## Non-transparent IP PDP Context Processing

The following figure and the text that follows describe how this configuration with a single source and destination context would be used by the system to process a non-transparent IP PDP context.

Figure 23. Non-transparent IP PDP Context Call Processing

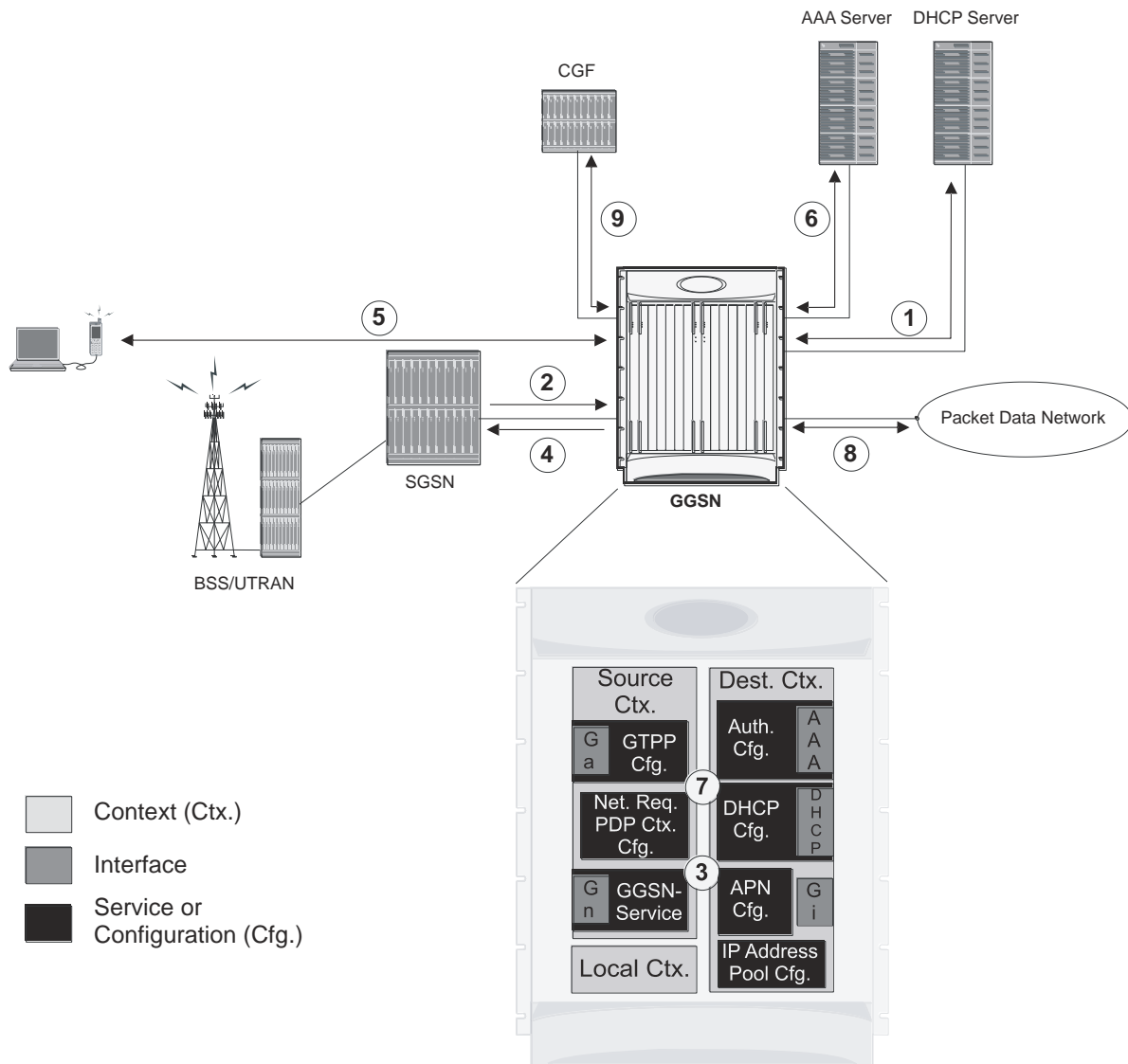


1. If the DHCP client mode is used for the dynamic assignment of IP addresses for subscriber PDP contexts, the system will retrieve addresses from the server over the DHCP interface during boot up and store them in cache memory.
2. A Create PDP Context Request message for a subscriber session is sent from the SGSN to the GGSN service over the Gn interface. The message contains information such as the PDP Type, APN, and charging characteristics.
3. The GGSN determines whether or not it is configured with an APN identical to the one specified in the message. If so, it determines how to process the session based on the configuration of the APN.
4. If the MS requires a dynamically assigned address, the GGSN assigns one from those stored in its memory cache.
5. If subscriber authentication is required, the GGSN authenticates the subscriber by communicating with a RADIUS server over the AAA interface.
6. The GGSN returns an affirmative Create PDP Context Response to the SGSN over the Gn interface.
7. The MS sends/receives data to/from the packet data network over the GGSN's PDN interface.
8. Upon termination of the subscriber session, the GGSN sends GGSN charging detail records to the CGF using GTPP over the Ga interface.

## PPP PDP Context Processing

The following figure and the following text describe how this configuration with a single source and destination context would be used by the system to process a PPP PDP context.

Figure 24. PPP PDP Context Call Processing



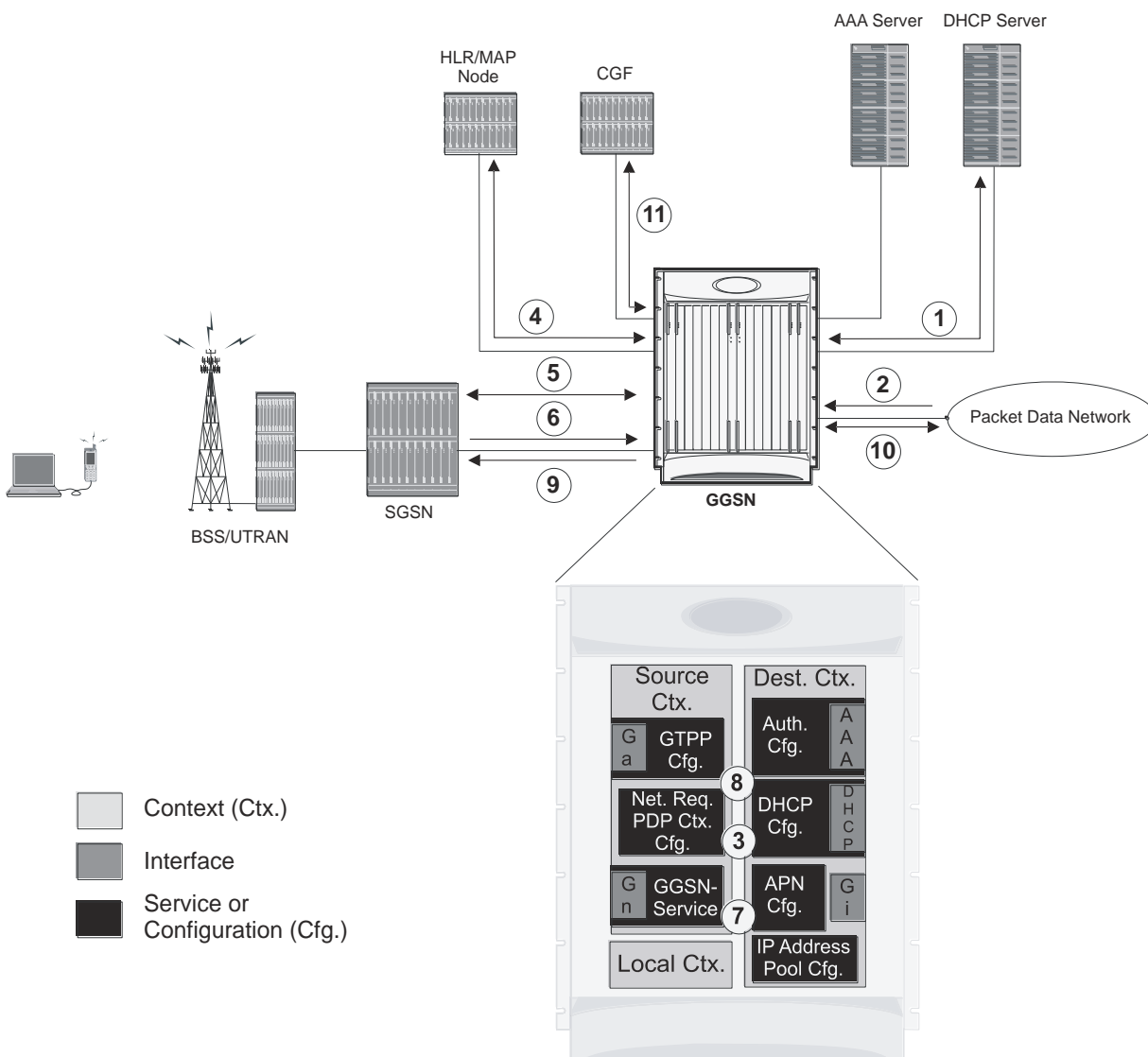
1. If the DHCP client mode is used for the dynamic assignment of IP addresses for subscriber PDP contexts, the system will retrieve addresses from the server over the DHCP interface during boot up and store them in cache memory.
2. A Create PDP Context Request message for a subscriber session is sent from the SGSN to the GGSN service over the Gn interface. The message contains information such as the PDP Type, APN, and charging characteristics.
3. The GGSN determines whether or not it is configured with an APN identical to the one specified in the message. If so, it determines how to process the session based on the configuration of the APN.
4. The GGSN returns an affirmative Create PDP Context Response to the SGSN over the Gn interface.
5. The MS and GGSN negotiate PPP.
6. The GGSN authenticates the subscriber as part of the PPP negotiation by communicating with a RADIUS server over the AAA interface.
7. Upon successful authentication, the GGSN assigns an IP address to the MS from one of those stored in its memory cache.
8. The MS sends/receives data to/from the packet data network over the GGSN's PDN interface.

9. Upon termination of the subscriber session, the GGSN sends GGSN charging detail records to the CGF using GTPP over the Ga interface.

## Network-requested PDP Context Processing

The following figure and the text that follows describe how this configuration with a single source and destination context would be used by the system to process a network-requested PDP context.

Figure 25. Network-requested PDP Context Call Processing



1. If the DHCP client mode is used for the dynamic assignment of IP addresses for subscriber PDP contexts, the system will retrieve addresses from the server over the DHCP interface during boot up and store them in cache memory.
2. An IP packet data unit (PDU) is received by the GGSN from the PDN.

3. The GGSN determines if it is configured to support network-initiated sessions. If so, it begins the Network-Requested PDP Context Activation procedure, otherwise it discards the packet.
4. The GGSN determines if the MS is reachable by communicating with the HLR through a MAP node over one of the Gn interfaces.
5. The GGSN works with the SGSN to activate the MS.
6. Once activated, the MS initiates a PDP context resulting in the sending of a Create PDP Context Request message from the SGSN to the GGSN service over the Gn interface. The message contains information such as the PDP Type, APN, and charging characteristics.
7. The GGSN determines whether or not it is configured with an APN identical to the one specified in the message. If so, it determines how to process the session based on the configuration of the APN.
8. If the MS requires a dynamically assigned address, the GGSN assigns one from those stored in its memory cache.
9. The GGSN returns an affirmative Create PDP Context Response to the SGSN over the Gn interface.
10. The MS sends/receives data to/from the packet data network over the GGSN's PDN interface.
11. Upon termination of the subscriber session, the GGSN sends GGSN charging detail records to the CGF using GTPP over the Ga interface.



# Chapter 4

## Mobile IP Configuration Examples

---

This chapter provides information for several configuration examples that can be implemented on the system to support Mobile IP (MIP) data services.



**Important:** This chapter does not discuss the configuration of the local context. Information about the local context can be found in *Command Line Reference*.



**Important:** When configuring Mobile IP take into account the MIP timing considerations discussed in *Mobile-IP and Proxy-MIP Timer Considerations* appendix.

---

## Example 1: Mobile IP Support Using the System as a GGSN/FA

For Mobile IP applications, the system can be configured to perform the function of a Gateway GPRS Support Node/Foreign Agent (GGSN/FA) and/or a Home Agent (HA). This example describes what is needed for and how the system performs the role of the GGSN/FA. Examples 2 and 3 provide information on using the system to provide HA functionality.

The system's GGSN/FA configuration for Mobile IP applications is best addressed with three contexts (one source, one AAA, and one Mobile IP destination) configured as shown in the figure that follows.



**Important:** A fourth context that serves as a destination context must also be configured if Reverse Tunneling is disabled in the FA service configuration. Reverse Tunneling is enabled by default.

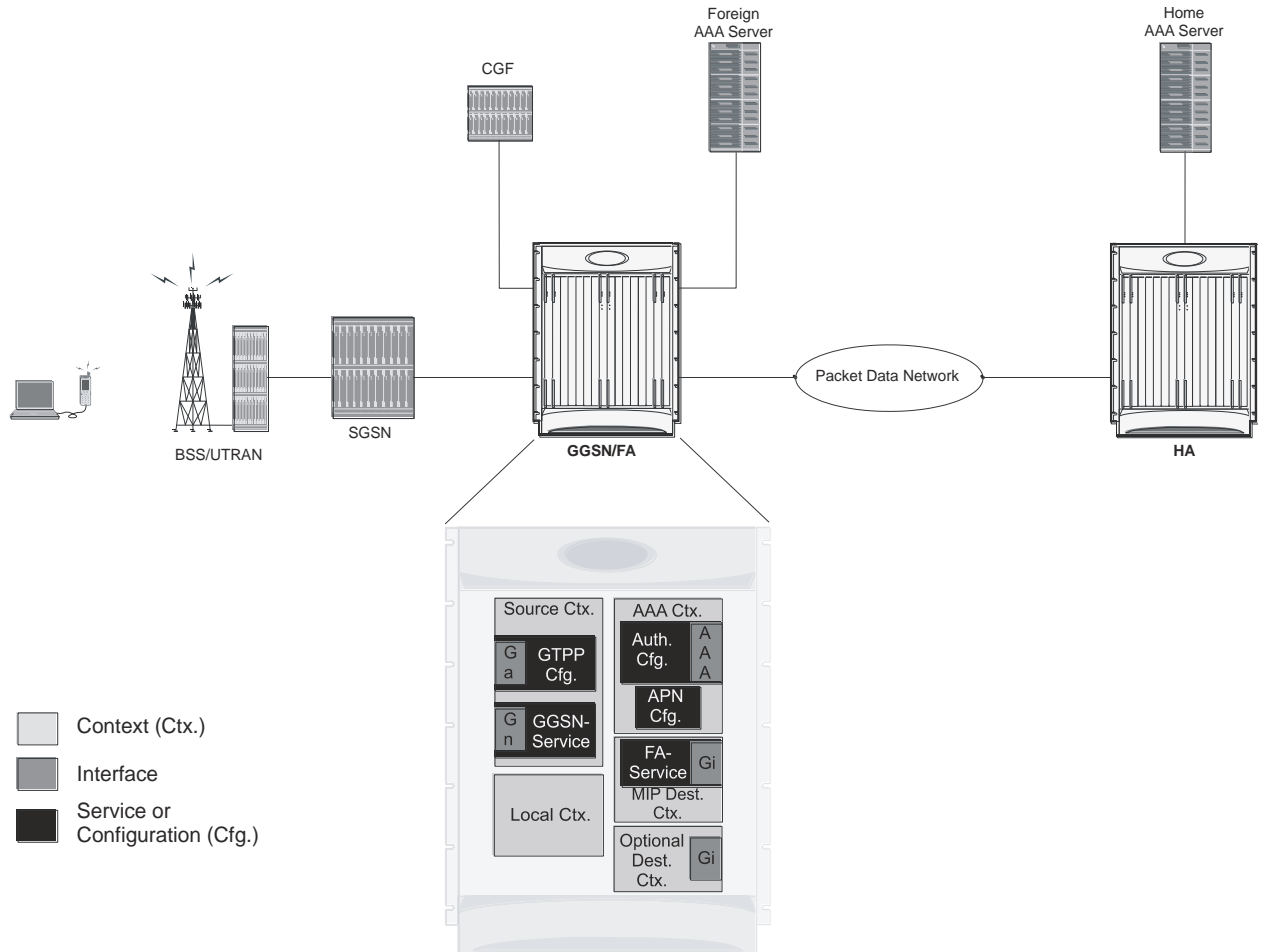
---

The source context will facilitate the GGSN service(s), and the Ga and Gn interfaces. The AAA context will be configured to provide foreign AAA functionality for subscriber PDP contexts and facilitate the AAA interfaces. The MIP destination context will facilitate the FA service(s) and the Gi interface(s) from the GGSN/FA to the HA.

The optional destination context will allow the routing of data from the mobile node to the packet data network by facilitating a packet data network (PDN) interface. This context will be used only if reverse tunneling is disabled.



Figure 26. Mobile IP Support using the system as a GGSN/FA



## Information Required

Prior to configuring the system as shown in this example, there is a minimum amount of information required. The following sections describe the information required to configure the source and destination contexts.

### Source Context Configuration

The following table lists the information that is required to configure the source context.

Table 3. Required Information for Source Context Configuration

Required Information	Description
Source context name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the source context will be recognized by the system. <b>NOTE:</b> The name of the source context should be the same as the name of the context in which the FA-context is configured if a separate system is being used to provide GGSN/FA functionality.

## ■ Example 1: Mobile IP Support Using the System as a GGSN/FA

Required Information	Description
Gn Interface Configuration	
Gn interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	These will be assigned to the Gn interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	An identification string from 1 to 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the source context and are used to bind logical Gn interfaces.
Gateway IP address	Used when configuring static routes from the Gn interface(s) to a specific network.
GGSN service Configuration	
GGSN service name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the GGSN service will be recognized by the system. Multiple names are needed if multiple GGSN services will be used.
Accounting context	The name of the context configured on the system in which the processing of GTPP accounting records is performed. The context name is an identification string from 1 to 79 characters (alpha and/or numeric). By default, the system attempts to use the same context as the one in which the GGSN service is configured.
UDP port number for GTPC traffic	The port used by the GGSN service and the SGSN for communicating GTPC sockets for GTPv1. The UDP port number can be any integer value from 1 to 65535. The default value is 2123.
Public Land Mobile Network (PLMN) Identifiers	<b>Mobile Country Code (MCC):</b> The MCC can be configured to any integer value from 0 to 999.
	<b>Mobile Network Code (MNC):</b> The MNC can be configured to any integer value from 0 to 999.
SGSN information (optional)	The GGSN can be configured with information about the SGSN(s) that it is to communicate with. This includes the SGSN's IP address and subnet mask and whether or not the SGSN is on a foreign PLMN. Multiple SGSNs can be configured.
GGSN charging characteristics (CC) (optional)	<p><b>Behavior Bits:</b> If charging characteristics will be configured on the GGSN, behavior bits for the following conditions can be configured:</p> <ul style="list-style-type: none"> <li>• GGSN use of the accounting server specified by the profile index</li> <li>• GGSN rejection of Create PDP Context Request messages</li> <li>• GGSN ceases sending accounting records</li> </ul> <p>Each value must be a unique bit from 1 to 12 to represent the 12 possible behavior bits allowed for in the standards. The default configuration is disabled (0).</p>

Required Information	Description
	<p><b>Profile Index:</b> If the GGSN's charging characteristics will be used for subscriber PDP contexts, profile indexes can be modified/configured for one or more of the following conditions:</p> <ul style="list-style-type: none"> <li>• The number of statistics container changes is met or exceeded causing an accounting record to be closed. The number can be configured from 1 to 15. The default is 4.</li> <li>• The up and/or downlink traffic volume limits are met or exceeded within a specific time interval causing a partial record to be generated. The up and downlink volumes can be configured from 0 to 1000000 octets. The interval can be configured from 60 to 40000000 seconds.</li> <li>• The up and/or downlink traffic volume limits are met or exceeded causing an accounting record to be closed. The up and downlink volumes can be configured from 100000 to 400000000 octets.</li> <li>• The number of SGSN switchovers is met or exceeded causing an accounting record to be closed. The number can be configured from 1 to 15. The default is 4.</li> <li>• Specific tariff times within a day are reached causing an accounting record to be closed. Up to four times can be configured using the hour of the day (1-24) and the minute (1-60).</li> </ul> <p>The system supports the configuration of up to 16 profile indexes numbered 0 through 15.</p>
PLMN policy	<p>The GGSN can be configured treat communications from unconfigured SGSNs in one of the following ways:</p> <ul style="list-style-type: none"> <li>• Treat the SGSN as if it is on a foreign PLMN</li> <li>• Treat the SGSN as if it is on a home PLMN</li> <li>• Reject communications from unconfigured SGSNs (default)</li> </ul>
Ga Interface Configuration	
Ga interface name	<p>An identification string from 1 to 79 characters (alpha and/or numeric) by which the interface will be recognized by the system.</p> <p>Multiple names are needed if multiple interfaces will be configured.</p>
IP address and subnet	<p>These will be assigned to the Ga interface.</p> <p>Multiple addresses and/or subnets are needed if multiple interfaces will be configured.</p>
Physical port number	<p>The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17.</p> <p>A single physical port can facilitate multiple interfaces.</p>
Physical port description	<p>An identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system.</p> <p>Multiple descriptions are needed if multiple ports will be used.</p> <p>Physical ports are configured within the source context and are used to bind logical Ga interfaces.</p>
Gateway IP address	Used when configuring static routes from the Ga interface(s) to a specific network.
GTP Configuration	
Charging gateway address	The IP address of the system's GGSN interface.

## ■ Example 1: Mobile IP Support Using the System as a GGSN/FA

Required Information	Description
CGF server information	<b>IP address:</b> The IP address of the CGF server to which the GGSN will send accounting information. Multiple CGFs can be configured.
	<b>Priority:</b> If more than one CGF is configured, this is the server's priority. It is used to determine the rotation order of the CGFs when sending accounting information. The priority can be configured to any integer value from 1 to 1000. The default is 1.
	<b>Maximum number of messages:</b> The maximum number of outstanding or unacknowledged GTPP messages allowed for the CGF. The maximum number can be configured to any integer value from 1 to 256. The default is 256.
GCDR optional fields	The following optional fields can be specified/configured in CDRs generated by the GGSN: <ul style="list-style-type: none"> <li>• diagnostics</li> <li>• duration-ms: the time specified in the mandatory Duration field is reported in milliseconds</li> <li>• local-record-sequence-number</li> <li>• plmn-id</li> </ul>

## AAA Context Configuration

The following table lists the information that is required to configure the AAA context.

Table 4. Required Information for AAA Context Configuration

Required Information	Description
AAA context name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the AAA context will be recognized by the system. <b>NOTE:</b> If a separate system is used to provide HA functionality, the AAA context name should match the name of the context in which the AAA functionality is configured on the HA machine.
APN Configuration	
APN name	An identification string by which the APN will be recognized by the system. The name can be from 1 to 62 alpha and/or numeric characters and is not case sensitive. It may also contain dots ( . ) and/or dashes ( - ). Multiple names are needed if multiple APNs will be used.
Accounting mode	Selects the accounting protocol. GTPP or RADIUS are supported. In addition, accounting can be completely disabled. The default is to perform accounting using GTPP. <b>NOTE:</b> The examples discussed in this chapter assume GTPP is used.
Authentication protocols used	Specifies how the system handles authentication: using a protocol (such as CHAP, PAP, or MSCHAP), or not requiring any authentication.

Required Information	Description
APN charging characteristics (CC) (optional)	Specifies whether or not the GGSN accepts the CC from the SGSN for home, visiting, and roaming subscribers. By default the GGSN accepts the CC from the SGSN for all three scenarios. If the GGSN is to use its own CC for any of these scenarios, then each scenario requires the specification of behavior bits and a profile index to use. <b>NOTE:</b> The profile index parameters are configured as part of the GGSN service.
Domain Name Service (DNS) information (optional)	If DNS will be used for the APN, IP addresses can be configured for primary and secondary DNS servers.
IP destination context name	The name of the system destination context to use for subscribers accessing the APN. If no name is specified, the system automatically uses the system context in which the APN is configured.
Maximum number of PDP contexts	The maximum number of PDP contexts that are supported for the APN. The maximum number can be configured to any integer value from 1 to 1500000. The default is 1000000.
PDP type	The type of PDP contexts supported by the APN. The type can be IPv4, IPv6, both IPv4 and IPv6, or PPP. IPv4 support is enabled by default.
Verification selection mode	The level of verification that will be used to ensure a MS's subscription to use the APN. The GGSN uses any of the following methods: <ul style="list-style-type: none"> <li>• No verification and MS supplies APN</li> <li>• No verification and SGSN supplies APN</li> <li>• Verified by SGSN (default)</li> </ul>
Mobile IP Configuration	<b>Home Agent IP Address:</b> The IP address of an HA with which the system will tunnel subscriber Mobile IP sessions. Configuring this information tunnels all subscriber Mobile IP PDP contexts facilitated by the APN to the same HA unless an individual subscriber profile provides an alternate HA address. Parameters stored in individual profiles supersede parameters provided by the APN.
	<b>Mobile IP Requirement:</b> The APN can be configured to require Mobile IP for all sessions it facilitates. Incoming PDP contexts that do/can not use Mobile IP are dropped.
AAA Interface Configuration	
AAA interface name	This is an identification string from 1 to 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	These will be assigned to the AAA interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	This is an identification string from 1 to 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are used to bind logical AAA interfaces.

## ■ Example 1: Mobile IP Support Using the System as a GGSN/FA

Required Information	Description
Gateway IP address	Used when configuring static routes from the AAA interface(s) to a specific network.
Foreign RADIUS Server Configuration	
Foreign RADIUS Authentication server	<b>IP Address:</b> Specifies the IP address of the Foreign RADIUS authentication server the system will communicate with to provide subscriber authentication functions. Multiple addresses are needed if multiple RADIUS servers. Foreign RADIUS servers are configured with in the source context. Multiple servers can be configured and each can be assigned a priority.
	<b>Shared Secret:</b> The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the RADIUS authentication server and the source context. A shared secret is needed for each configured RADIUS server.
	<b>UDP Port Number:</b> Specifies the port used by the source context and the RADIUS authentication server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1812.
Foreign RADIUS Accounting server (optional)	<b>IP Address:</b> Specifies the IP address of the foreign RADIUS accounting server that the source context will communicate with to provide subscriber accounting functions. Multiple addresses are needed if multiple RADIUS servers will be configured. RADIUS accounting servers are configured within the source context. Multiple servers can be configured and each assigned a priority.
	<b>Shared Secret:</b> The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the foreign RADIUS accounting server and the source context. A shared secret is needed for each configured RADIUS server.
	<b>UDP Port Number:</b> Specifies the port used by the source context and the foreign RADIUS Accounting server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1813.
RADIUS attribute NAS Identifier	Specifies the name by which the source context will be identified in the Access-Request message(s) it sends to the RADIUS server. The name must be from 1 to 32 alpha and/or numeric characters and is case sensitive.
RADIUS NAS IP address	Specifies the IP address of the system's AAA interface. A secondary address can be optionally configured.

## Mobile IP Destination Context Configuration

The following table lists the information that is required to configure the Mobile IP destination context.

Table 5. Required Information for Mobile IP Destination Context Configuration

Required Information	Description
----------------------	-------------

Required Information	Description
Mobile IP Destination context name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the Mobile IP destination context will be recognized by the system. <b>NOTE:</b> For this configuration, the destination context name should <b>not</b> match the domain name of a specific domain. It should, however, match the name of the context in which the HA service is configured if a separate system is used to provide HA functionality.
Gi Interface Configuration	
Gi interface name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. Gi interfaces are configured in the destination context.
IP address and subnet	These will be assigned to the Gi interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description(s)	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions will be needed if multiple ports will be used. Physical ports are configured within the destination context and are used to bind logical Gi interfaces.
Gateway IP address(es)	Used when configuring static routes from the Gi interface(s) to a specific network.
FA Service Configuration	
FA service name	This is an identification string between 1 and 63 characters (alpha and/or numeric) by which the FA service will be recognized by the system. Multiple names are needed if multiple FA services will be used. FA services are configured in the destination context.
UDP port number for Mobile IP traffic	Specifies the port used by the FA service and the HA for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 434.
Security Parameter Index (indices) Information	<b>HA IP address:</b> Specifies the IP address of the HAs with which the FA service communicates. The FA service allows the creation of a security profile that can be associated with a particular HA.
	<b>Index:</b> Specifies the shared SPI between the FA service and a particular HA. The SPI can be configured to any integer value between 256 and 4294967295. Multiple SPIs can be configured if the FA service is to communicate with multiple HAs.
	<b>Secrets:</b> Specifies the shared SPI secret between the FA service and the HA. The secret can be between 1 and 127 characters (alpha and/or numeric). An SPI secret is required for each SPI configured.
	<b>Hash-algorithm:</b> Specifies the algorithm used to hash the SPI and SPI secret. The possible algorithms that can be configured are MD5 per RFC 1321 and keyed-MD5 per RFC 2002. The default is hmac-md5. A hash-algorithm is required for each SPI configured.
FA agent advertisement lifetime	Specifies the time (in seconds) that an FA agent advertisement remains valid in the absence of further advertisements. The time can be configured to any integer value between 1 and 65535. The default is 9000.

## ■ Example 1: Mobile IP Support Using the System as a GGSN/FA

Required Information	Description
Number of allowable unanswered FA advertisements	Specifies the number of unanswered agent advertisements that the FA service will allow during call setup before it will reject the session. The number can be any integer value between 1 and 65535. The default is 5.
Maximum mobile-requested registration lifetime allowed	Specifies the longest registration lifetime that the FA service will allow in any Registration Request message from the mobile node. The lifetime is expressed in seconds and can be configured between 1 and 65534. An infinite registration lifetime can be configured by disabling the timer. The default is 600 seconds.
Registration reply timeout	Specifies the amount of time that the FA service will wait for a Registration Reply from an HA. The time is measured in seconds and can be configured to any integer value between 1 and 65535. The default is 7.
Number of simultaneous registrations	Specifies the number of simultaneous Mobile IP sessions that will be supported for a single subscriber. The maximum number of sessions is 3. The default is 1. <b>NOTE:</b> The system will only support multiple Mobile IP sessions per subscriber if the subscriber's mobile node has a static IP address.
Mobile node re-registration requirements	Specifies how the system should handle authentication for mobile node re-registrations. The FA service can be configured to always require authentication or not. If not, the initial registration and de-registration will still be handled normally.
Maximum registration lifetime	Specifies the longest registration lifetime that the HA service will allow in any Registration Request message from the mobile node. The time is measured in seconds and can be configured to any integer value between 1 and 65535. An infinite registration lifetime can also be configured by disabling the timer. The default is 600.
Maximum number of simultaneous bindings	Specifies the maximum number of "care-of" addresses that can simultaneously be bound for the same user as identified by NAI and Home address. The number can be configured to any integer value between 1 and 5. The default is 3.

## Optional Destination Context Configuration

The following table lists the information required to configure the optional destination context. As discussed previously, this context is required if: 1) reverse tunneling is disabled in the FA service, or 2) if access control lists (ACLs) are used



**Important:** If ACLs are used, the destination context would only consist of the ACL configuration. Interface configuration would not be required.

Table 6. Required Information for Destination Context Configuration

Required Information	Description
Destination context name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the destination context will be recognized by the system. <b>NOTE:</b> For this configuration, the destination context name should <b>not</b> match the domain name of a specific domain.
PDN Interface Configuration	



Required Information	Description
PDN interface name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. PDN interfaces are configured in the destination context.
IP address and subnet	These will be assigned to the PDN interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the destination context and are used to bind logical PDN interfaces.
Gateway IP address(es)	Used when configuring static routes from the PDN interface(s) to a specific network.

## How This Configuration Works

The following figure and the text that follows describe how this configuration with a single source and destination context would be used by the system to process a Mobile IP data call.

[illegible]

1. A Create PDP Context Request message for a subscriber session is sent from the SGSN to the GGSN service over the Gn interface. The message contains information such as the PDP Type, APN, and charging characteristics.
2. The GGSN determines whether or not it is configured with an APN identical to the one specified in the message. If so, it determines how to process the session based on the configuration of the APN. In this case, it is determined that Mobile IP must be used. From the APM configuration, the system also determines the context in which the FA service is configured.
3. If subscriber authentication is required, the GGSN authenticates the subscriber by communicating with a RADIUS server over the AAA interface.
4. The GGSN returns an affirmative Create PDP Context Response to the SGSN over the Gn interface. The home address assigned to the mobile as part of the response is 0.0.0.0 indicating that it will be reset with a Home address after the PDP context activation procedure.
5. The FA component of the GGSN sends a Agent Advertisement message to the MS. The message contains the FA parameters needed by the mobile such as one or more card-of addresses. The message is sent as an IP limited broadcast message (i.e. destination address 255.255.255.255), however only on the requesting MS's TEID to avoid broadcast over the radio interface.

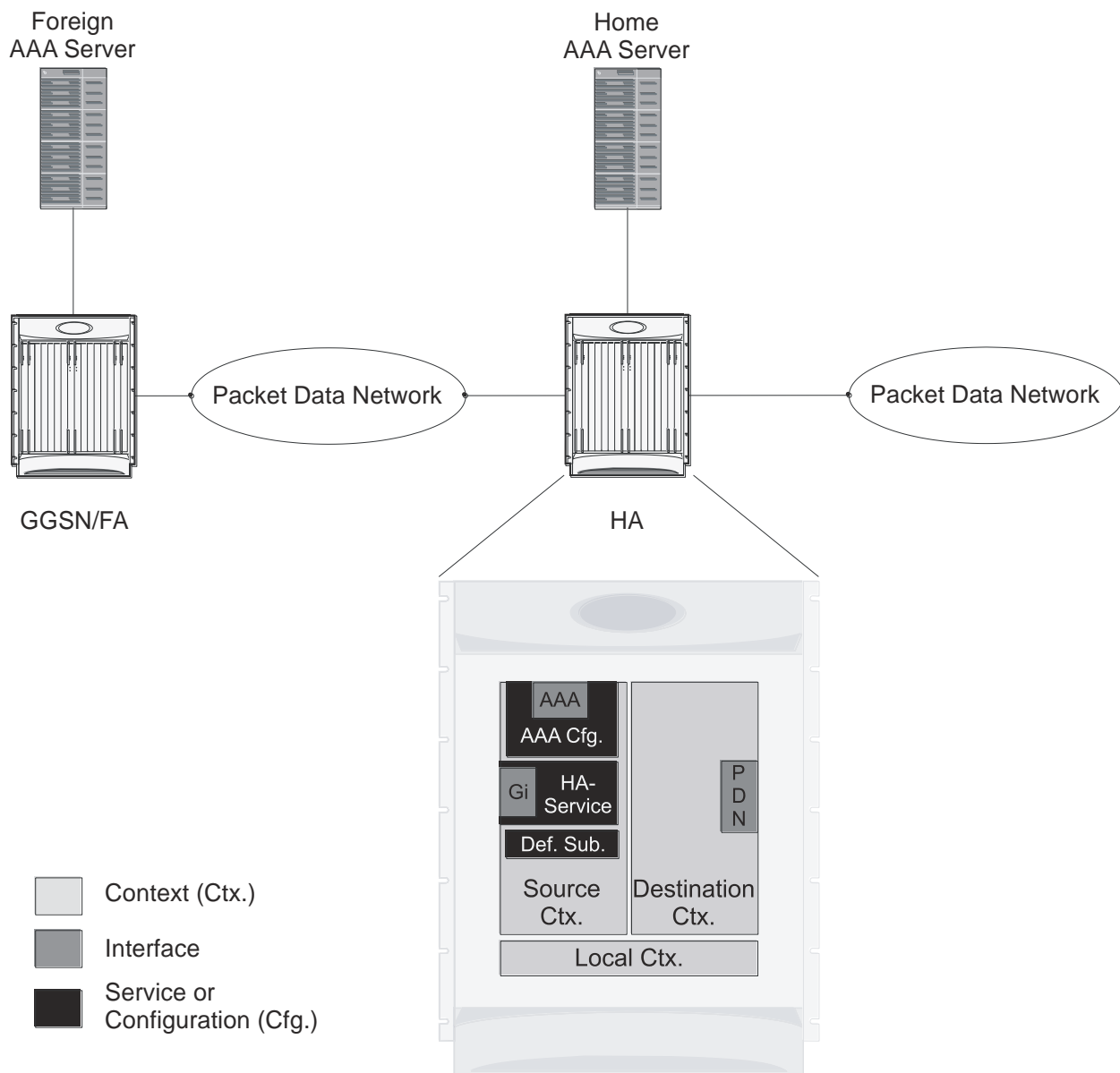
6. The MS sends a Mobile IP Registration request to the GGSN/FA. This message includes either the MS's static home address or it can request a temporary address by sending 0.0.0.0 as its home address. Additionally, the request must always include the Network Access Identifier (NAI) in a Mobile-Node-NAI Extension.
7. The FA forwards the registration request from the MS to the HA while the MS's home address or NAI and TEID are stored by the GGSN. In response the HA sends a registration response to the FA containing the address assigned to the MS.
8. The FA extracts the home address assigned to the MS by the HA from the response and the GGSN updates the associated PDP context. The FA then forwards it to the MS (identified by either the home address or the NAI and TEID).
9. The GGSN issues a PDP context modification procedure to the SGSN in order to update the PDP address for the MS.
10. The MS sends/receives data to/from the packet data network over the GGSN's PDN interface.
11. Upon termination of the subscriber session, the GGSN sends GGSN charging detail records to the CGF using GTPP over the Ga interface.

## Example 2: Mobile IP Support Using the System as an HA

The system supports both Simple and Mobile IP. For Mobile IP applications, the system can be configured to perform the function of a GGSN/FA and/or a HA. This example describes what is needed for and how the system performs the role of the HA. Example number 1 provides information on using the system to provide GGSN/FA functionality.

The system's HA configuration for Mobile IP applications requires that at least two contexts (one source and one destination) be configured as shown in the following figure.

Figure 28. Mobile IP Support Using the system as an HA



The source context will facilitate the HA service(s), the Gi interfaces from the FA, and the AAA interfaces. The source context will also be configured to provide Home AAA functionality for subscriber sessions. The destination context will facilitate the PDN interface(s).

## Information Required

Prior to configuring the system as shown in this example, there is a minimum amount of information required. The following sections describe the information required to configure the source and destination contexts.

### Source Context Configuration

The following table lists the information that is required to configure the source context.

**Table 7. Required Information for Source Context Configuration**

Required Information	Description
Source context name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the source context will be recognized by the system.
Gi Interface Configuration	
Gi interface name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. Gi interfaces are configured in the destination context.
IP address and subnet	These will be assigned to the Gi interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description(s)	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions will be needed if multiple ports will be used. Physical ports are configured within the destination context and are used to bind logical Gi interfaces.
Gateway IP address	Used when configuring static routes from the Gi interface(s) to a specific network.
HA service Configuration	
HA service name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the HA service will be recognized by the system. Multiple names are needed if multiple HA services will be used. HA services are configured in the destination context.
UDP port number for Mobile IP traffic	The port used by the HA service and the FA for communications. The UDP port number can be any integer value from 1 to 65535. The default value is 434.

## ■ Example 2: Mobile IP Support Using the System as an HA

Required Information	Description
Mobile node re-registration requirements	<p>Specifies how the system should handle authentication for mobile node re-registrations. The HA service can be configured as follows:</p> <ul style="list-style-type: none"> <li>• Always require authentication</li> <li>• Never require authentication</li> </ul> <p><b>NOTE:</b> The initial registration and de-registration will still be handled normally)</p> <ul style="list-style-type: none"> <li>• Never look for mn-aaa extension</li> <li>• Not require authentication but will authenticate if mn-aaa extension present.</li> </ul>
FA-to-HA Security Parameter Index Information	<p><b>FA IP address:</b> The HA service allows the creation of a security profile that can be associated with a particular FA. This specifies the IP address of the FA that the HA service will be communicating with. Multiple FA addresses are needed if the HA will be communicating with multiple FAs.</p>
	<p><b>Index:</b> Specifies the shared SPI between the HA service and a particular FA. The SPI can be configured to any integer value between 256 and 4294967295. Multiple SPIs can be configured if the HA service is to communicate with multiple FAs.</p>
	<p><b>Secret:</b> Specifies the shared SPI secret between the HA service and the FA. The secret can be between 1 and 127 characters (alpha and/or numeric). An SPI secret is required for each SPI configured.</p>
	<p><b>Hash-algorithm:</b> Specifies the algorithm used to hash the SPI and SPI secret. The possible algorithms that can be configured are MD5 per RFC 1321 and keyed-MD5 per RFC 2002. The default algorithm is <b>hmac-md5</b>. A hash-algorithm is required for each SPI configured.</p>
Mobile Node Security Parameter Index Information	<p><b>Index:</b> Specifies the shared SPI between the HA service and a particular FA. The SPI can be configured to any integer value between 256 and 4294967295. Multiple SPIs can be configured if the HA service is to communicate with multiple FAs.</p>
	<p><b>Secret:</b> Specifies the shared SPI secret between the HA service and the FA. The secret can be between 1 and 127 characters (alpha and/or numeric). An SPI secret is required for each SPI configured.</p>
	<p><b>Hash-algorithm:</b> Specifies the algorithm used to hash the SPI and SPI secret. The possible algorithms that can be configured are MD5 per RFC 1321 and keyed-MD5 per RFC 2002. The default algorithm is <b>hmac-md5</b>. A hash-algorithm is required for each SPI configured.</p>
	<p><b>Replay-protection process:</b> Specifies how protection against replay-attacks is implemented. The possible processes are nonce and timestamp. The default is timestamp with a tolerance of 60 seconds. A replay-protection process is required for each mobile node-to-HA SPI configured.</p>
Maximum registration lifetime	<p>Specifies the longest registration lifetime that the HA service will allow in any Registration Request message from the mobile node. The time is measured in seconds and can be configured to any integer value between 1 and 65535. An infinite registration lifetime can also be configured by disabling the timer. The default is 600.</p>
Maximum number of simultaneous bindings	<p>Specifies the maximum number of “care-of” addresses that can simultaneously be bound for the same user as identified by NAI and Home address. The number can be configured to any integer value between 1 and 5. The default is 3.</p>
AAA Interface Configuration	

Required Information	Description
AAA interface name	This is an identification string from 1 to 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. AAA interfaces will be configured in the source context.
IP address and subnet	These will be assigned to the AAA interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	This is an identification string from 1 to 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are used to bind logical AAA interfaces.
Gateway IP address	Used when configuring static routes from the AAA interface(s) to a specific network.
Home RADIUS Server Configuration	
Home RADIUS Authentication server	<b>IP Address:</b> Specifies the IP address of the home RADIUS authentication server the system will communicate with to provide subscriber authentication functions. Multiple addresses are needed if multiple RADIUS servers. Home RADIUS servers are configured with in the source context. Multiple servers can be configured and each can be assigned a priority.
	<b>Shared Secret:</b> The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the RADIUS authentication server and the source context. A shared secret is needed for each configured RADIUS server.
	<b>UDP Port Number:</b> Specifies the port used by the source context and the RADIUS authentication server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1812.
Home RADIUS Accounting server (optional)	<b>IP Address:</b> Specifies the IP address of the home RADIUS accounting server that the source context will communicate with to provide subscriber accounting functions. Multiple addresses are needed if multiple RADIUS servers will be configured. RADIUS accounting servers are configured within the source context. Multiple servers can be configured and each assigned a priority.
	<b>Shared Secret:</b> The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the home RADIUS accounting server and the source context. A shared secret is needed for each configured RADIUS server.
	<b>UDP Port Number:</b> Specifies the port used by the source context and the home RADIUS Accounting server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1813.
RADIUS attribute NAS Identifier	Specifies the name by which the source context will be identified in the Access-Request message(s) it sends to the RADIUS server. The name must be from 1 to 32 alpha and/or numeric characters and is case sensitive.
RADIUS NAS IP address	Specifies the IP address of the system's AAA interface. A secondary address can be optionally configured.

## ■ Example 2: Mobile IP Support Using the System as an HA

Required Information	Description
Default Subscriber Configuration	
“Default” subscriber’s IP context name	Specifies the name of the egress context on the system that facilitates the Gi interfaces. <b>NOTE:</b> For this configuration, the IP context name should be identical to the name of the destination context.

## Destination Context Configuration

The following table lists the information required to configure the destination context.

**Table 8. Required Information for Destination Context Configuration**

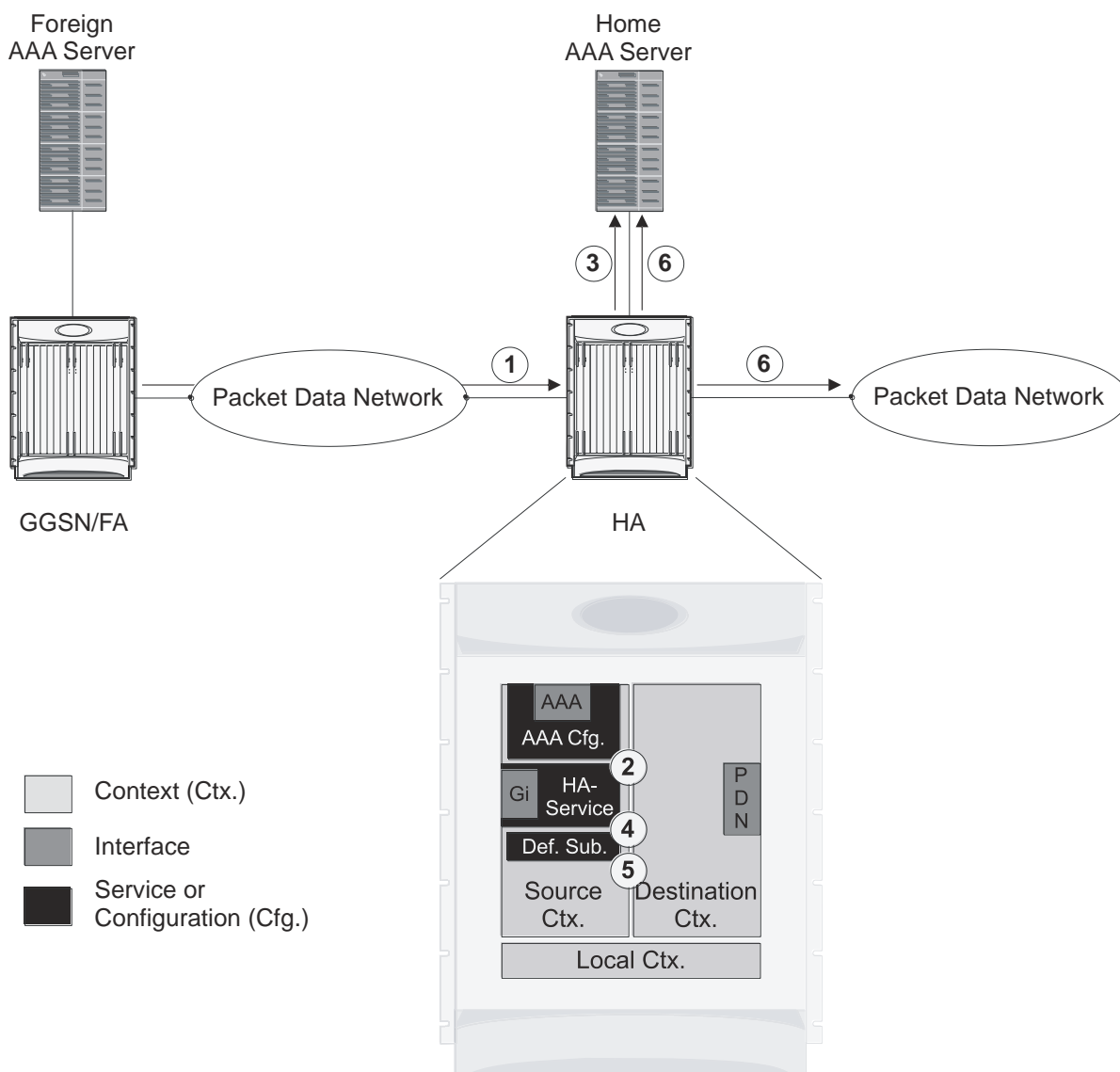
Required Information	Description
Destination context name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the destination context will be recognized by the system. <b>NOTE:</b> For this configuration, the destination context name should <b>not</b> match the domain name of a specific domain.
PDN Interface Configuration	
PDN interface name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. PDN interfaces are configured in the destination context.
IP address and subnet	These will be assigned to the PDN interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the destination context and are used to bind logical PDN interfaces.
Gateway IP address(es)	Used when configuring static routes from the PDN interface(s) to a specific network.
IP Address Pool Configuration	
IP address pool name	Each IP address pool is identified by a name. The pool name can be between 1 and 31 alpha and/or numeric characters and is case sensitive. IP address pools are configured in the destination context(s). Multiple address pools can be configured within a single context.
IP pool addresses	An initial address and a subnet, or a starting address and an ending address, are required for each configured pool. The pool will then consist of every possible address within the subnet, or all addresses from the starting address to the ending address. The pool can be configured as public, private, or static.



## How This Configuration Works

The following figure and the text that follows describe how this configuration with a single source and destination context would be used by the system to process a Mobile IP data call.

Figure 29. Call Processing When Using the system as an HA



1. A subscriber session from the FA is received by the HA service over the Gi interface.
2. The HA service determines which context to use to provide AAA functionality for the session. This process is described in the *How the System Selects Contexts* section located in the *Understanding the System Operation and Configuration* chapter of the *System Administration Guide*.

## ■ Example 2: Mobile IP Support Using the System as an HA

For this example, the result of this process is that the HA service determined that AAA functionality should be provided by the *Source* context.

3. The system then communicates with the Home AAA server specified in the Source context's AAA configuration to authenticate the subscriber.
4. Upon successful authentication, the *Source* context determines which egress context to use for the subscriber session. This process is described in the *How the System Selects Contexts* section located in the *Understanding the System Operation and Configuration* chapter of the *System Administration Guide*.

For this example, the system determines that the egress context is the Destination context based on the configuration of the *Default* subscriber.

5. An IP address is assigned to the subscriber's mobile node from an IP address pool configured in the destination context. This IP address is used for the duration of the session and then be returned to the pool.
6. Data traffic for the subscriber session is then routed through the PDN interface in the *Destination* context.
7. Accounting messages for the session are sent to the AAA server over the AAA interface.

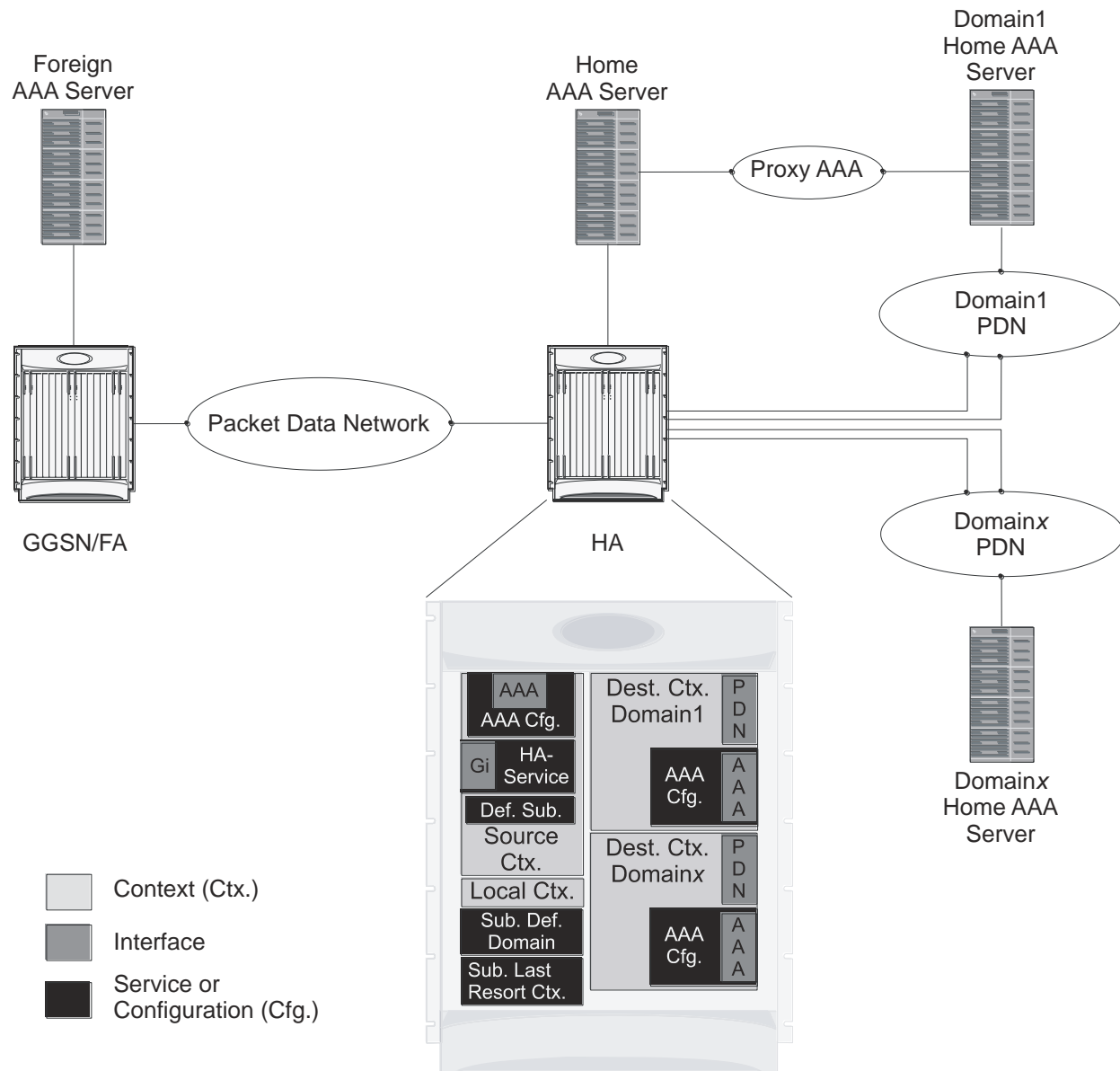
## Example 3: HA Using a Single Source Context and Multiple Outsourced Destination Contexts

The system allows the wireless carrier to easily generate additional revenue by providing the ability to configure separate contexts that can then be leased or outsourced to various enterprises or ISPs, each having a specific domain.

In order to perform the role of an HA and support multiple outsourced domains, the system must be configured with at least one source context and multiple destination contexts as shown in the following figure. The AAA servers could be owned/maintained by either the carrier or the domain. If they are owned by the domain, the carrier will have to receive the AAA information via proxy.

### Example 3: HA Using a Single Source Context and Multiple Outsourced Destination Contexts

Figure 30. The system as an HA Using a Single Source Context and Multiple Outsourced Destination Contexts



The source context will facilitate the HA service(s), and the Gi interface(s) to the FA(s). The source context will also be configured with AAA interface(s) and to provide Home AAA functionality for subscriber sessions. The destination contexts will each be configured to facilitate PDN interfaces. In addition, because each of the destination contexts can be outsourced to different domains, they will also be configured with AAA interface(s) and to provide AAA functionality for that domain.

In addition to the source and destination contexts, there are additional system-level AAA parameters that must be configured.

## Information Required

Prior to configuring the system as shown in this example, there is a minimum amount of information required. The following sections describe the information required to configure the source and destination contexts.

### Source Context Configuration

The following table lists the information that is required to configure the source context.

**Table 9. Required Information for Source Context Configuration**

Required Information	Description
Source context name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the source context will be recognized by the system.
Gi Interface Configuration	
Gi interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. Gi interfaces are configured in the destination context.
IP address and subnet	These will be assigned to the Gi interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	An identification string from 1 to 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the source context and are used to bind logical Gn interfaces.
Gateway IP address	Used when configuring static routes from the Gi interface(s) to a specific network.
HA service Configuration	
HA service name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the HA service will be recognized by the system. Multiple names are needed if multiple HA services will be used. HA services are configured in the destination context.
UDP port number for Mobile IP traffic	The port used by the HA service and the FA for communications. The UDP port number and can be any integer value from 1 to 65535. The default value is 434.

## ■ Example 3: HA Using a Single Source Context and Multiple Outsourced Destination Contexts

Required Information	Description
Mobile node re-registration requirements	<p>Specifies how the system should handle authentication for mobile node re-registrations. The HA service can be configured as follows:</p> <ul style="list-style-type: none"> <li>• Always require authentication</li> <li>• Never require authentication</li> </ul> <p><b>NOTE:</b> The initial registration and de-registration will still be handled normally)</p> <ul style="list-style-type: none"> <li>• Never look for mn-aaa extension</li> <li>• Not require authentication but will authenticate if mn-aaa extension present.</li> </ul>
FA-to-HA Security Parameter Index Information	<p><b>FA IP address:</b> The HA service allows the creation of a security profile that can be associated with a particular FA. This specifies the IP address of the FA that the HA service will be communicating with. Multiple FA addresses are needed if the HA will be communicating with multiple FAs.</p>
	<p><b>Index:</b> Specifies the shared SPI between the HA service and a particular FA. The SPI can be configured to any integer value between 256 and 4294967295. Multiple SPIs can be configured if the HA service is to communicate with multiple FAs.</p>
	<p><b>Secret:</b> Specifies the shared SPI secret between the HA service and the FA. The secret can be between 1 and 127 characters (alpha and/or numeric). An SPI secret is required for each SPI configured.</p>
	<p><b>Hash-algorithm:</b> Specifies the algorithm used to hash the SPI and SPI secret. The possible algorithms that can be configured are MD5 per RFC 1321 and keyed-MD5 per RFC 2002. The default algorithm is <b>hmac-md5</b>. A hash-algorithm is required for each SPI configured.</p>
Mobile Node Security Parameter Index Information	<p><b>Index:</b> Specifies the shared SPI between the HA service and a particular FA. The SPI can be configured to any integer value between 256 and 4294967295. Multiple SPIs can be configured if the HA service is to communicate with multiple FAs.</p>
	<p><b>Secret:</b> Specifies the shared SPI secret between the HA service and the FA. The secret can be between 1 and 127 characters (alpha and/or numeric). An SPI secret is required for each SPI configured.</p>
	<p><b>Hash-algorithm:</b> Specifies the algorithm used to hash the SPI and SPI secret. The possible algorithms that can be configured are MD5 per RFC 1321 and keyed-MD5 per RFC 2002. The default algorithm is <b>hmac-md5</b>. A hash-algorithm is required for each SPI configured.</p>
	<p><b>Replay-protection process:</b> Specifies how protection against replay-attacks is implemented. The possible processes are nonce and timestamp. The default is timestamp with a tolerance of 60 seconds. A replay-protection process is required for each mobile node-to-HA SPI configured.</p>
Maximum registration lifetime	<p>Specifies the longest registration lifetime that the HA service will allow in any Registration Request message from the mobile node. The time is measured in seconds and can be configured to any integer value between 1 and 65535. An infinite registration lifetime can also be configured by disabling the timer. The default is 600.</p>
Maximum number of simultaneous bindings	<p>Specifies the maximum number of “care-of” addresses that can simultaneously be bound for the same user as identified by NAI and Home address. The number can be configured to any integer value between 1 and 5. The default is 3.</p>
AAA Interface Configuration	

Required Information	Description
AAA interface name	This is an identification string from 1 to 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. AAA interfaces will be configured in the source context.
IP address and subnet	These will be assigned to the AAA interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	This is an identification string from 1 to 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are used to bind logical AAA interfaces.
Gateway IP address	Used when configuring static routes from the AAA interface(s) to a specific network.
Home RADIUS Server Configuration	
Home RADIUS Authentication server	<b>IP Address:</b> Specifies the IP address of the home RADIUS authentication server the system will communicate with to provide subscriber authentication functions. Multiple addresses are needed if multiple RADIUS servers. Home RADIUS servers are configured with in the source context. Multiple servers can be configured and each can be assigned a priority.
	<b>Shared Secret:</b> The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the RADIUS authentication server and the source context. A shared secret is needed for each configured RADIUS server.
	<b>UDP Port Number:</b> Specifies the port used by the source context and the RADIUS authentication server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1812.
Home RADIUS Accounting server (optional)	<b>IP Address:</b> Specifies the IP address of the home RADIUS accounting server that the source context will communicate with to provide subscriber accounting functions. Multiple addresses are needed if multiple RADIUS servers will be configured. RADIUS accounting servers are configured within the source context. Multiple servers can be configured and each assigned a priority.
	<b>Shared Secret:</b> The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the home RADIUS accounting server and the source context. A shared secret is needed for each configured RADIUS server.
	<b>UDP Port Number:</b> Specifies the port used by the source context and the home RADIUS Accounting server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1813.
RADIUS attribute NAS Identifier	Specifies the name by which the source context will be identified in the Access-Request message(s) it sends to the RADIUS server. The name must be from 1 to 32 alpha and/or numeric characters and is case sensitive.
RADIUS NAS IP address	Specifies the IP address of the system's AAA interface. A secondary address can be optionally configured.

## ■ Example 3: HA Using a Single Source Context and Multiple Outsourced Destination Contexts

Required Information	Description
Default Subscriber Configuration	
“Default” subscriber’s IP context name	Specifies the name of the egress context on the system that facilitates the Gi interfaces. <b>NOTE:</b> For this configuration, the IP context name should be identical to the name of the destination context.

## Destination Context Configuration

The following table lists the information required to configure the destination context. This information will be required for each domain.

**Table 10. Required Information for Destination Context Configuration**

Required Information	Description
Destination context name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the destination context will be recognized by the system. <b>NOTE:</b> For this configuration, the destination context name should <b>not</b> match the domain name of a specific domain.
PDN Interface Configuration	
PDN interface name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. PDN interfaces are configured in the destination context.
IP address and subnet	These will be assigned to the PDN interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the destination context and are used to bind logical PDN interfaces.
Gateway IP address(es)	Used when configuring static routes from the PDN interface(s) to a specific network.
IP Address Pool Configuration (optional)	
IP address pool name	Each IP address pool is identified by a name. The pool name can be between 1 and 31 alpha and/or numeric characters and is case sensitive. IP address pools are configured in the destination context(s). Multiple address pools can be configured within a single context.
IP pool addresses	An initial address and a subnet, or a starting address and an ending address, are required for each configured pool. The pool will then consist of every possible address within the subnet, or all addresses from the starting address to the ending address. The pool can be configured as public, private, or static.
AAA Interface Configuration	



Required Information	Description
AAA interface name	This is an identification string from 1 to 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	These will be assigned to the AAA interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	This is an identification string from 1 to 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are used to bind logical AAA interfaces.
Gateway IP address	Used when configuring static routes from the AAA interface(s) to a specific network.
RADIUS Server Configuration	
RADIUS Authentication server	<b>IP Address:</b> Specifies the IP address of the RADIUS authentication server the system will communicate with to provide subscriber authentication functions. Multiple addresses are needed if multiple RADIUS servers. Foreign RADIUS servers are configured with in the source context. Multiple servers can be configured and each can be assigned a priority.
	<b>Shared Secret:</b> The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the RADIUS authentication server and the source context. A shared secret is needed for each configured RADIUS server.
	<b>UDP Port Number:</b> Specifies the port used by the source context and the RADIUS authentication server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1812.
RADIUS Accounting server (optional)	<b>IP Address:</b> Specifies the IP address of the RADIUS accounting server that the source context will communicate with to provide subscriber accounting functions. Multiple addresses are needed if multiple RADIUS servers will be configured. RADIUS accounting servers are configured within the source context. Multiple servers can be configured and each assigned a priority.
	<b>Shared Secret:</b> The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the RADIUS accounting server and the source context. A shared secret is needed for each configured RADIUS server.
	<b>UDP Port Number:</b> Specifies the port used by the source context and the RADIUS Accounting server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1813.
RADIUS attribute NAS Identifier	Specifies the name by which the source context will be identified in the Access-Request message(s) it sends to the RADIUS server. The name must be from 1 to 32 alpha and/or numeric characters and is case sensitive.
RADIUS NAS IP address	Specifies the IP address of the system's AAA interface. A secondary address can be optionally configured.

### ■ Example 3: HA Using a Single Source Context and Multiple Outsourced Destination Contexts

## System-Level AAA Configuration

The following table lists the information that is required to configure the system-level AAA parameters.

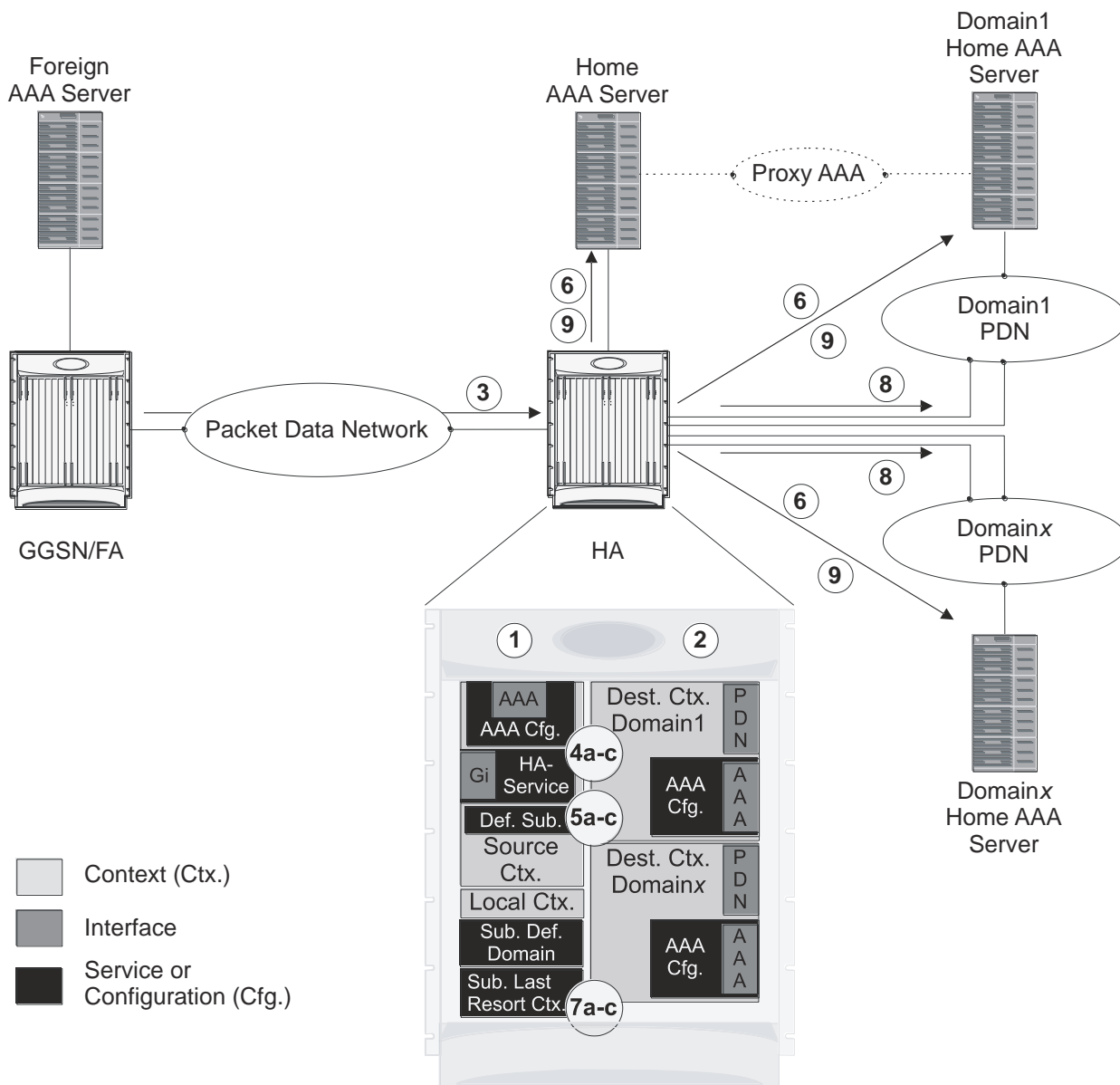
Table 11. Required Information for System-Level AAA Configuration

Required Information	Description
Subscriber default domain name	Specifies the name of a context that can provide AAA functions in the event that the domain-part of the username is missing or poorly formed. This parameter will be applied to all subscribers if their domain cannot be determined from their username regardless of what domain they are trying to access. <b>NOTE:</b> The default domain name can be the same as the source context.
Subscriber Last-resort context	Specifies the name of a context that can provide AAA functions in the event that the domain-part of the username was present but does not match the name of a configured destination context .This parameter will be applied to all subscribers if their specified domain does not match a configured destination context regardless of what domain they are trying to access. <b>NOTE:</b> The last-resort context name can be the same as the source context.
Subscriber username format	Specifies the format of subscriber usernames as to whether or not the username or domain is specified first and the character that separates them. The possible separator characters are: <ul style="list-style-type: none"> <li>• @</li> <li>• %</li> <li>• -</li> <li>• \</li> <li>• #</li> <li>• /</li> </ul> Up to six username formats can be specified. The default is <i>username @</i> . <b>NOTE:</b> The username string is searched from right to left for the separator character. Therefore, if there are one or more separator characters in the string, only the first one that is recognized is considered the actual separator. For example, if the default username format was used, then for the username string <i>user1@enterprise@isp1</i> , the system resolves to the username <i>user1@enterprise</i> with domain <i>isp1</i> .

## How This Configuration Works

The following figure and the text that follows describe how this configuration with a single source and destination context would be used by the system to process a Mobile IP data call.

**Figure 31. Call Processing When Using the system as an HA with a Single Source Context and Multiple Outsourced Destination Contexts**



1. The system-level AAA settings were configured as follows:
  - Subscriber default domain name = *Domainx*
  - Subscriber username format = *username@*
  - No subscriber last-resort context name was configured
2. The subscriber IP context names were configured as follows:
  - Within the *Source* context, the IP context name was configured as *Domainx*
  - Within the *Domainx* context, the IP context name was configured as *Domainx*
3. Sessions are received by the HA service from the FA over the Gi interface for *subscriber1@Domain1*, *subscriber2*, and *subscriber3@Domain37*.

## ■ Example 3: HA Using a Single Source Context and Multiple Outsourced Destination Contexts

4. The HA service attempts to determine the domain names for each session.
  - For *subscriber1*, the HA service determines that a domain name is present and is *Domain1*.
  - For *subscriber2*, the HA service determines that no domain name is present.
  - For *subscriber3*, the HA service determines that a domain name is present and is *Domain37*.
5. The HA service determines which context to use to provide AAA functionality for the session. This process is described in the *How the System Selects Contexts* section located in the *Understanding the System Operation and Configuration* chapter of the *System Administration Guide*.
  - For *subscriber1*, the HA service determines that a context was configured with a name (*Domain1*) that matches the domain name specified in the username string. Therefore, *Domain1* is used.
  - For *subscriber2*, the HA service determines that *Domainx* is configured as the default domain name. Therefore, *Domainx* is used.
  - For *subscriber3*, the HA service determines that no context is configured that matches the domain name (*Domain37*) specified in the username string. Because no **last-resort** context name was configured, the *Source* context is used.
6. The system then communicates with the Home AAA server specified in the Source context's AAA configuration to authenticate the subscriber.
7. Upon successful authentication of all three subscribers, the HA service determines which destination context to use for each of the subscriber sessions. This process is described in the *How the System Selects Contexts* section located in the *Understanding the System Operation and Configuration* chapter of the *System Administration Guide*.
  - For *subscriber1*, the HA service receives the *SN-VPN-NAME* or *SNI-VPN-NAME* attribute equal to *Domain1* as part of the Authentication Accept message from the AAA server on *Domain1*'s network. Therefore, *Domain1* is used as the destination context.
  - For *subscriber2*, the HA service determines that the *SN-VPN-NAME* or *SNI-VPN-NAME* attribute was not returned with the Authentication Accept response, and determines the subscriber IP context name configured within the *Domainx* context. Therefore, the *Domainx* context is used as the destination context.
  - For *subscriber3*, the HA service determines that the *SN-VPN-NAME* or *SNI-VPN-NAME* attribute was not returned with the Authentication Accept response, and determines the subscriber IP context name configured within the *Source* context. Therefore, the *Source* context is used as the destination context.
8. Data traffic for the subscriber session is then routed through the PDN interface in the each subscriber's destination context.
9. Accounting messages for the session are sent to the AAA server over the appropriate AAA interface.


# Chapter 5


## GGSN and Mobile IP Service in a Single System Configuration Example

---

This chapter provides information for several configuration examples that can be implemented on the system to support GGSN and Mobile IP data services in a single system.

---

 **Important:** This chapter does not discuss the configuration of the local context. Information about the local context can be found in *System Administration Guide*.

 **Important:** When configuring Mobile IP take into account the MIP timing considerations discussed in *Mobile-IP and Proxy-MIP Timer Considerations*.

---

## Using the System as Both a GGSN/FA and an HA

The system supports both GGSN and Mobile IP functionality. For Mobile IP applications, the system can be configured to perform the function of a Gateway GPRS Support Node/Foreign Agent (GGSNSN/FA) and/or a Home Agent (HA). This example describes what is needed for and how a single system simultaneously supports both of these functions.

In order to support GGSN, FA, and HA functionality, the system must be configured with at least one source context and at least two destination contexts as shown in the following figure.

The source context facilitates the following:

- GGSN service(s) and Gn interface to the Service GPRS Support Node (SGSN)
- GPRS Tunneling Protocol Prime (GTPP) configuration and Ga interface to the Charging Gateway Function (CGF)

The destination context facilitates the following:

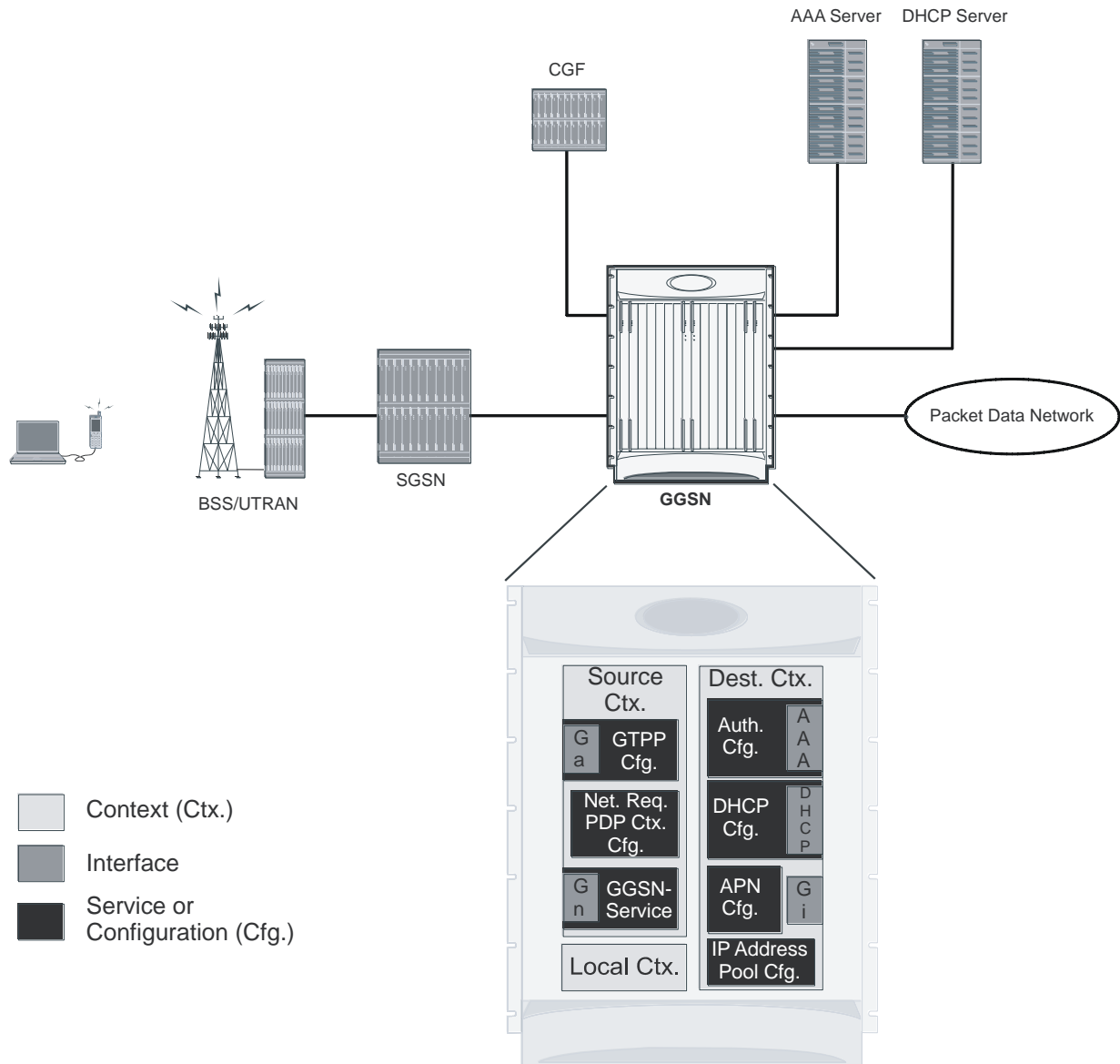
- Access Point Name (APN) configuration
- RADIUS authentication configuration and the interface to the authentication server
- DHCP configuration and the interface to the DHCP server
- IP address pools
- Gi interface to the packet data network (PDN)

The Mobile IP destination context facilitates the following:

- FA Service(s)
- HA Service(s)
- Gi interface to the packet data network (PDN)
- ICC interface facilitating communication between the FA and HA services.

This configuration supports IP (transparent and non-transparent) and PPP PDP contexts as well as network requested PDP contexts. In addition, Mobile IP and Proxy Mobile IP are supported for IP PDP contexts.

Figure 32. Simple and Mobile IP Support Within a Single System



## Information Required

Prior to configuring the system as shown in this example, there is a minimum amount of information required. The following sections describe the required information to configure the source and destination contexts.

### Source Context Configuration

The following table lists the information that is required to configure the source context.

Table 12. Required Information for Source Context Configuration

Required Information	Description
Source context name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the source context will be recognized by the system.
Gn Interface Configuration	
Gn interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	These will be assigned to the Gn interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	An identification string from 1 to 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the source context and are used to bind logical Gn interfaces.
Gateway IP address	Used when configuring static routes from the Gn interface(s) to a specific network.
GGSN service Configuration	
GGSN service name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the GGSN service will be recognized by the system. Multiple names are needed if multiple GGSN services will be used.
Accounting context	The name of the context configured on the system in which the processing of GTPP accounting records is performed. The context name is an identification string from 1 to 79 characters (alpha and/or numeric). By default, the system attempts to use the same context as the one in which the GGSN service is configured.
UDP port number for GTPC traffic	The port used by the GGSN service and the SGSN for communicating GTPC sockets for GTPv1. The UDP port number can be any integer value from 1 to 65535. The default value is 2123.
Public Land Mobile Network (PLMN) Identifiers	<b>Mobile Country Code (MCC):</b> The MCC can be configured to any integer value from 0 to 999.
	<b>Mobile Network Code (MNC):</b> The MNC can be configured to any integer value from 0 to 999.
SGSN information (optional)	The GGSN can be configured with information about the SGSN(s) that it is to communicate with. This includes the SGSN's IP address and subnet mask and whether or not the SGSN is on a foreign PLMN. Multiple SGSNs can be configured.



Required Information	Description
GGSN charging characteristics (CC) (optional)	<p><b>Behavior Bits:</b> If charging characteristics will be configured on the GGSN, behavior bits for the following conditions can be configured:</p> <ul style="list-style-type: none"> <li>• GGSN use of the accounting server specified by the profile index</li> <li>• GGSN rejection of Create PDP Context Request messages</li> <li>• GGSN ceases sending accounting records</li> </ul> <p>Each value must be a unique bit from 1 to 12 to represent the 12 possible behavior bits allowed for in the standards. The default configuration is disabled (0).</p> <p><b>Profile Index:</b> If the GGSN's charging characteristics will be used for subscriber PDP contexts, profile indexes can be modified/configured for one or more of the following conditions:</p> <ul style="list-style-type: none"> <li>• The number of statistics container changes is met or exceeded causing an accounting record to be closed. The number can be configured from 1 to 15. The default is 4.</li> <li>• The up and/or downlink traffic volume limits are met or exceeded within a specific time interval causing a partial record to be generated. The up and downlink volumes can be configured from 0 to 1000000 octets. The interval can be configured from 60 to 40000000 seconds.</li> <li>• The up and/or downlink traffic volume limits are met or exceeded causing an accounting record to be closed. The up and downlink volumes can be configured from 100000 to 4000000000 octets.</li> <li>• The number of SGSN switchovers is met or exceeded causing an accounting record to be closed. The number can be configured from 1 to 15. The default is 4.</li> <li>• Specific tariff times within a day are reached causing an accounting record to be closed. Up to four times can be configured using the hour of the day (1-24) and the minute (1-60).</li> <li>• Prepaid accounting can be disabled for a specified profile index.</li> </ul> <p>The system supports the configuration of up to 16 profile indexes numbered 0 through 15</p>
PLMN policy	<p>The GGSN can be configured treat communications from unconfigured SGSNs in one of the following ways:</p> <ul style="list-style-type: none"> <li>• Treat the SGSN as if it is on a foreign PLMN</li> <li>• Treat the SGSN as if it is on a home PLMN</li> <li>• Reject communications from unconfigured SGSNs (default)</li> </ul>
Ga Interface Configuration	
Ga interface name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	These will be assigned to the Ga interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.

## ■ Using the System as Both a GGSN/FA and an HA

Required Information	Description
Physical port description	An identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the source context and are used to bind logical Ga interfaces.
Gateway IP address	Used when configuring static routes from the Ga interface(s) to a specific network.
GTPP Configuration	
Charging gateway address	The IP address of the system's GGSN interface.
CGF server information	<b>IP address:</b> The IP address of the CGF server to which the GGSN will send accounting information. Multiple CGFs can be configured.
	<b>Priority:</b> If more than one CGF is configured, this is the server's priority. It is used to determine the rotation order of the CGFs when sending accounting information. The priority can be configured to any integer value from 1 to 1000. The default is 1.
	<b>Maximum number of messages:</b> The maximum number of outstanding or unacknowledged GTPP messages allowed for the CGF. The maximum number can be configured to any integer value from 1 to 256. The default is 256.
GCDR optional fields	The following optional fields can be specified/configured in CDRs generated by the GGSN: <ul style="list-style-type: none"> <li>• diagnostics</li> <li>• duration-ms (the time specified in the mandatory Duration field is reported in milliseconds)</li> <li>• local-record-sequence-number</li> <li>• plmn-id</li> </ul>
Network Requested PDP Context Support Configuration (optional)	
Activation Requirements	<b>IP address:</b> The static IP address of the mobile station's for which network-requested PDP context activation will be supported. Up to 1000 addresses can be configured.
	<b>Destination context name:</b> The name of the destination context configured on the system that contains the IP address pool containing the mobile station's static address.
	<b>International Mobile Subscriber Identity (IMSI):</b> The IMSI of the mobile station.
	<b>APN:</b> The name of the access point that will be passed to the SGSN by the GGSN for the mobile station.
GSN-map node	Communications with the HLR from the GGSN go through a GSN-map node that performs the protocol conversion from GTPC to SS7. The IP address of the map node must be configured. Only one GSN-map node can be configured per source context.

## Destination Context Configuration

The following table lists the information that is required to configure the destination context.

Table 13. Required Information for Destination Context Configuration

Required Information	Description
Destination context name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the destination context will be recognized by the system. <b>NOTE:</b> For this configuration, the destination context name should <b>not</b> match the domain name of a specific APN.
APN Configuration	
APN name	An identification string by which the APN will be recognized by the system. The name can be from 1 to 62 alpha and/or numeric characters and is not case sensitive. It may also contain dots ( . ) and/or dashes ( - ). Multiple names are needed if multiple APNs will be used.
Accounting mode	Selects the accounting protocol. GTPP or RADIUS are supported. In addition, accounting can be completely disabled. The default is to perform accounting using GTPP. <b>NOTE:</b> The examples discussed in this chapter assumes GTPP is used.
Authentication protocols used	Specifies how the system handles authentication: using a protocol (such as CHAP, PAP, or MSCHAP), or not requiring any authentication.
APN charging characteristics (CC) (optional)	Specifies whether or not the GGSN accepts the CC from the SGSN for home, visiting, and roaming subscribers. By default the GGSN accepts the CC from the SGSN for all three scenarios. If the GGSN is to use its own CC for any of these scenarios, then each scenario requires the specification of behavior bits and a profile index to use. <b>NOTE:</b> The profile index parameters are configured as part of the GGSN service.
Domain Name Service (DNS) information (optional)	If DNS will be used for the APN, IP addresses can be configured for primary and secondary DNS servers.
IP address allocation method	Specifies how sessions facilitated by this APN will receive an IP address. IP addresses can be assigned using one of the following methods: <ul style="list-style-type: none"> <li>• <b>Dynamic:</b> Address can be dynamically assigned from one of the sources: <ul style="list-style-type: none"> <li>• <b>Dynamic Host Control Protocol (DHCP) server:</b> The system can be configured to act as a DHCP proxy and receive address from the server in advance and assign them as needed or it can relay DHCP messages from the MS.</li> <li>• <b>Local address pools</b> The system can be configured with local address pools.</li> </ul> </li> <li>• <b>Static:</b> MS IP addresses can be permanently assigned.</li> </ul> By default, the system is configured to either dynamically assign addresses from a local pool and/or allow static addresses.
IP address pool name	If addresses will be dynamically assigned from a locally configured private pool, the name of the pool must be configured. If no name is configured, the system will automatically use any configured public pool.
IP destination context name	The name of the system destination context to use for subscribers accessing the APN. When supporting Mobile IP, this is the name of the context containing the FA service configuration. If no name is specified, the system automatically uses the system context in which the APN is configured.
Maximum number of PDP contexts	The maximum number of PDP contexts that are supported for the APN. The maximum number can be configured to any integer value from 1 to 1000000. The default is 1000000.

# Using the System as Both a GGSN/FA and an HA

Required Information	Description
PDP type	The maximum number of PDP contexts that are supported for the APN. The maximum number can be configured to any integer value from 1 to 1500000. The default is 1000000.
Verification selection mode	The level of verification that will be used to ensure a MS's subscription to use the APN. The GGSN uses any of the following methods: <ul style="list-style-type: none"> <li>No verification and MS supplies APN</li> <li>No verification and SGSN supplies APN</li> <li>Verified by SGSN (default)</li> </ul>
Mobile IP Configuration	<b>Home Agent IP Address:</b> The IP address of an HA with which the system will tunnel subscriber Mobile IP sessions. Configuring this information tunnels all subscriber Mobile IP PDP contexts facilitated by the APN to the same HA unless an individual subscriber profile provides an alternate HA address. Parameters stored in individual profiles supersede parameters provided by the APN.
	<b>Mobile IP Requirement:</b> The APN can be configured to require Mobile IP for all sessions it facilitates. Incoming PDP contexts that do/can not use Mobile IP are dropped.
DHCP Interface Configuration (optional)	
DHCP interface name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	These will be assigned to the DHCP interface and be bound to the DHCP service. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Gateway IP address	Used when configuring static routes from the DHCP interface(s) to a specific network.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	An identification string from 1 to 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the source context and are used to bind logical DHCP interfaces.
DHCP Service Configuration (optional)	
DHCP Service Name	This is an identification string between 1 and 63 characters (alpha and/or numeric) by which the DHCP service will be recognized by the system. Multiple names are needed if multiple GGSN services will be used.
DHCP Server Information	The IP address of each DHCP server that the system is to communicate with must be configured .Multiple servers can be configured. If multiple servers are configured, each can be assigned a priority from 1 to 1000. The default priority is 1.

Required Information	Description
Lease Duration	<p>Specifies the minimum and maximum allowable lease times that are accepted in responses from DHCP servers.</p> <ul style="list-style-type: none"> <li><b>Minimum Lease Time:</b> Measured in seconds and can be configured to any integer value from 600 to 3600. The default is 600 seconds.</li> <li><b>Maximum Lease Time:</b> Measured in seconds and can be configured to any integer value from 10800 to 4294967295. The default is 86400 seconds.</li> </ul>
AAA Interface Configuration	
AAA interface name	<p>This is an identification string from 1 to 79 characters (alpha and/or numeric) by which the interface will be recognized by the system.</p> <p>Multiple names are needed if multiple interfaces will be configured.</p>
IP address and subnet	<p>These will be assigned to the AAA interface.</p> <p>Multiple addresses and/or subnets are needed if multiple interfaces will be configured.</p>
Physical port number	<p>This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17.</p> <p>A single physical port can facilitate multiple interfaces.</p>
Physical port description	<p>This is an identification string from 1 to 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system.</p> <p>Multiple descriptions are needed if multiple ports will be used.</p> <p>Physical ports are used to bind logical AAA interfaces.</p>
Gateway IP address	<p>Used when configuring static routes from the AAA interface(s) to a specific network.</p>
RADIUS Server Configuration	
RADIUS Authentication server	<p><b>IP Address:</b> Specifies the IP address of the RADIUS authentication server the system will communicate with to provide subscriber authentication functions.</p> <p>Multiple addresses are needed if multiple RADIUS servers will be configured. If multiple servers are configured, each can be assigned a priority.</p>
	<p><b>Shared Secret:</b> The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the RADIUS authentication server and the source context. A shared secret is needed for each configured RADIUS server.</p>
	<p><b>UDP Port Number:</b> Specifies the port used by the source context and the RADIUS authentication server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1812.</p>
RADIUS Accounting server (optional)	<p><b>IP Address:</b> Specifies the IP address of the RADIUS accounting server that the source context will communicate with to provide subscriber accounting functions.</p> <p>Multiple addresses are needed if multiple RADIUS servers will be configured. RADIUS accounting servers are configured within the source context.</p> <p>Multiple servers can be configured and each assigned a priority.</p>
	<p><b>Shared Secret:</b> The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the RADIUS accounting server and the source context. A shared secret is needed for each configured RADIUS server.</p>
	<p><b>UDP Port Number:</b> Specifies the port used by the source context and the RADIUS Accounting server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1813.</p>

## ■ Using the System as Both a GGSN/FA and an HA

Required Information	Description
RADIUS attribute NAS Identifier	Specifies the name by which the source context will be identified in the Access-Request message(s) it sends to the RADIUS server. The name must be from 1 to 32 alpha and/or numeric characters and is case sensitive.
RADIUS NAS IP address	Specifies the IP address of the system's AAA interface. A secondary address can be optionally configured.
Gi Interface Configuration	
Gi interface name	This is an identification string from 1 to 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. Gi interfaces are configured in the destination context.
IP address and subnet	These will be assigned to the Gi interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description(s)	This is an identification string from 1 to 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions will be needed if multiple ports will be used. Physical ports are configured within the destination context and are used to bind logical Gi interfaces.
Gateway IP address(es)	Used when configuring static routes from the Gi interface(s) to a specific network.
IP Address Pool Configuration	
IP address pool name(s)	This is an identification string from 1 to 31 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions will be needed if multiple ports will be used.
Pool addresses, subnet mask and type	The pool can consist of either of the following: <ul style="list-style-type: none"> <li>• An entire subnet configured using the initial address and the subnet mask</li> <li>• A range of addresses configured using the first and last IP addresses in the range</li> </ul> The pool can be configured as public, private, or static. Public pools can also be assigned a priority.

## Mobile IP Destination Context Configuration

The following table lists the information that is required to configure the destination context.

Table 14. Required Information for Mobile IP Destination Context Configuration

Required Information	Description
----------------------	-------------

Required Information	Description
Mobile IP Destination context name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the Mobile IP destination context will be recognized by the system. <b>NOTE:</b> For this configuration, the destination context name should <b>not</b> match the domain name of a specific domain. It should, however, match the name of the context in which the HA service is configured if a separate system is used to provide HA functionality.
ICC Interface Configuration	
ICC interface name	The intra-context communication (ICC) interface is configured to allow FA and HA services configured within the same context to communicate with each other. The ICC interface name is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. ICC interface(s) are configured in the same destination context as the FA and HA services.
IP address and subnet	These will be assigned to the ICC interface(s). Multiple addresses (at least one per service) on the same subnet will be needed to assign to the same ICC interface.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the destination context and are used to bind logical ICC interfaces.
Gi Interface Configuration	
Gi interface name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. Gi interfaces are configured in the destination context.
IP address and subnet	These will be assigned to the Gi interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description(s)	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions will be needed if multiple ports will be used. Physical ports are configured within the destination context and are used to bind logical Gi interfaces.
Gateway IP address(es)	Used when configuring static routes from the Gi interface(s) to a specific network.
IP Address Pool Configuration (optional)	

# Using the System as Both a GGSN/FA and an HA

Required Information	Description
IP address pool name(s)	If IP address pools will be configured in the destination context(s), names or identifiers will be needed for them. The pool name can be between 1 and 31 alpha and/or numeric characters and is case sensitive.
IP pool addresses	An initial address and a subnet, or a starting address and an ending address, are required for each configured pool. The pool will then consist of every possible address within the subnet, or all addresses from the starting address to the ending address. The pool can be configured as public, private, or static.
FA Service Configuration	
FA service name	This is an identification string between 1 and 63 characters (alpha and/or numeric) by which the FA service will be recognized by the system .Multiple names are needed if multiple FA services will be used. FA services are configured in the destination context.
UDP port number for Mobile IP traffic	Specifies the port used by the FA service and the HA for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 434.
Security Parameter Index (indices) Information	<b>HA IP address:</b> Specifies the IP address of the HAs with which the FA service communicates. The FA service allows the creation of a security profile that can be associated with a particular HA.
	<b>Index:</b> Specifies the shared SPI between the FA service and a particular HA. The SPI can be configured to any integer value between 256 and 4294967295. Multiple SPIs can be configured if the FA service is to communicate with multiple HAs.
	<b>Secrets:</b> Specifies the shared SPI secret between the FA service and the HA. The secret can be between 1 and 127 characters (alpha and/or numeric). An SPI secret is required for each SPI configured.
	<b>Hash-algorithm:</b> Specifies the algorithm used to hash the SPI and SPI secret. The possible algorithms that can be configured are MD5 per RFC 1321 and keyed-MD5 per RFC 2002. The default is hmac-md5. A hash-algorithm is required for each SPI configured.
FA agent advertisement lifetime	Specifies the time (in seconds) that an FA agent advertisement remains valid in the absence of further advertisements. The time can be configured to any integer value between 1 and 65535. The default is 9000.
Number of allowable unanswered FA advertisements	Specifies the number of unanswered agent advertisements that the FA service will allow during call setup before it will reject the session. The number can be any integer value between 1 and 65535. The default is 5.
Maximum mobile-requested registration lifetime allowed	Specifies the longest registration lifetime that the FA service will allow in any Registration Request message from the mobile node. The lifetime is expressed in seconds and can be configured between 1 and 65534. An infinite registration lifetime can be configured by disabling the timer. The default is 600 seconds.
Registration reply timeout	Specifies the amount of time that the FA service will wait for a Registration Reply from an HA. The time is measured in seconds and can be configured to any integer value between 1 and 65535. The default is 7.
Number of simultaneous registrations	Specifies the number of simultaneous Mobile IP sessions that will be supported for a single subscriber. The maximum number of sessions is 3. The default is 1. <b>NOTE:</b> The system will only support multiple Mobile IP sessions per subscriber if the subscriber's mobile node has a static IP address.



Required Information	Description
Mobile node re-registration requirements	Specifies how the system should handle authentication for mobile node re-registrations. The FA service can be configured to always require authentication or not. If not, the initial registration and de-registration will still be handled normally.
HA service Configuration	
HA service name	This is an identification string between 1 and 63 characters (alpha and/or numeric) by which the HA service will be recognized by the system. Multiple names are needed if multiple HA services will be used. HA services are configured in the destination context.
UDP port number for Mobile IP traffic	Specifies the port used by the HA service and the FA for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 434.
Mobile node re-registration requirements	Specifies how the system should handle authentication for mobile node re-registrations. The HA service can be configured as follows: <ul style="list-style-type: none"> <li>Always require authentication</li> <li>Never require authentication</li> </ul> <p><b>NOTE:</b> The initial registration and de-registration will still be handled normally)</p> <ul style="list-style-type: none"> <li>Never look for mn-aaa extension</li> <li>Not require authentication but will authenticate if mn-aaa extension present.</li> </ul>
FA-to-HA Security Parameter Index Information	<b>FA IP address:</b> The HA service allows the creation of a security profile that can be associated with a particular FA. This specifies the IP address of the FA that the HA service will be communicating with. Multiple FA addresses are needed if the HA will be communicating with multiple FAs.
	<b>Index:</b> Specifies the shared SPI between the HA service and a particular FA. The SPI can be configured to any integer value between 256 and 4294967295. Multiple SPIs can be configured if the HA service is to communicate with multiple FAs.
	<b>Secret:</b> Specifies the shared SPI secret between the HA service and the FA. The secret can be between 1 and 127 characters (alpha and/or numeric). An SPI secret is required for each SPI configured.
	<b>Hash-algorithm:</b> Specifies the algorithm used to hash the SPI and SPI secret. The possible algorithms that can be configured are MD5 per RFC 1321 and keyed-MD5 per RFC 2002. The default algorithm is <b>hmac-md5</b> . A hash-algorithm is required for each SPI configured.
Mobile Node Security Parameter Index Information	<b>Index:</b> Specifies the shared SPI between the HA service and a particular FA. The SPI can be configured to any integer value between 256 and 4294967295. Multiple SPIs can be configured if the HA service is to communicate with multiple FAs.
	<b>Secret:</b> Specifies the shared SPI secret between the HA service and the FA. The secret can be between 1 and 127 characters (alpha and/or numeric). An SPI secret is required for each SPI configured.
	<b>Hash-algorithm:</b> Specifies the algorithm used to hash the SPI and SPI secret. The possible algorithms that can be configured are MD5 per RFC 1321 and keyed-MD5 per RFC 2002. The default algorithm is <b>hmac-md5</b> . A hash-algorithm is required for each SPI configured.

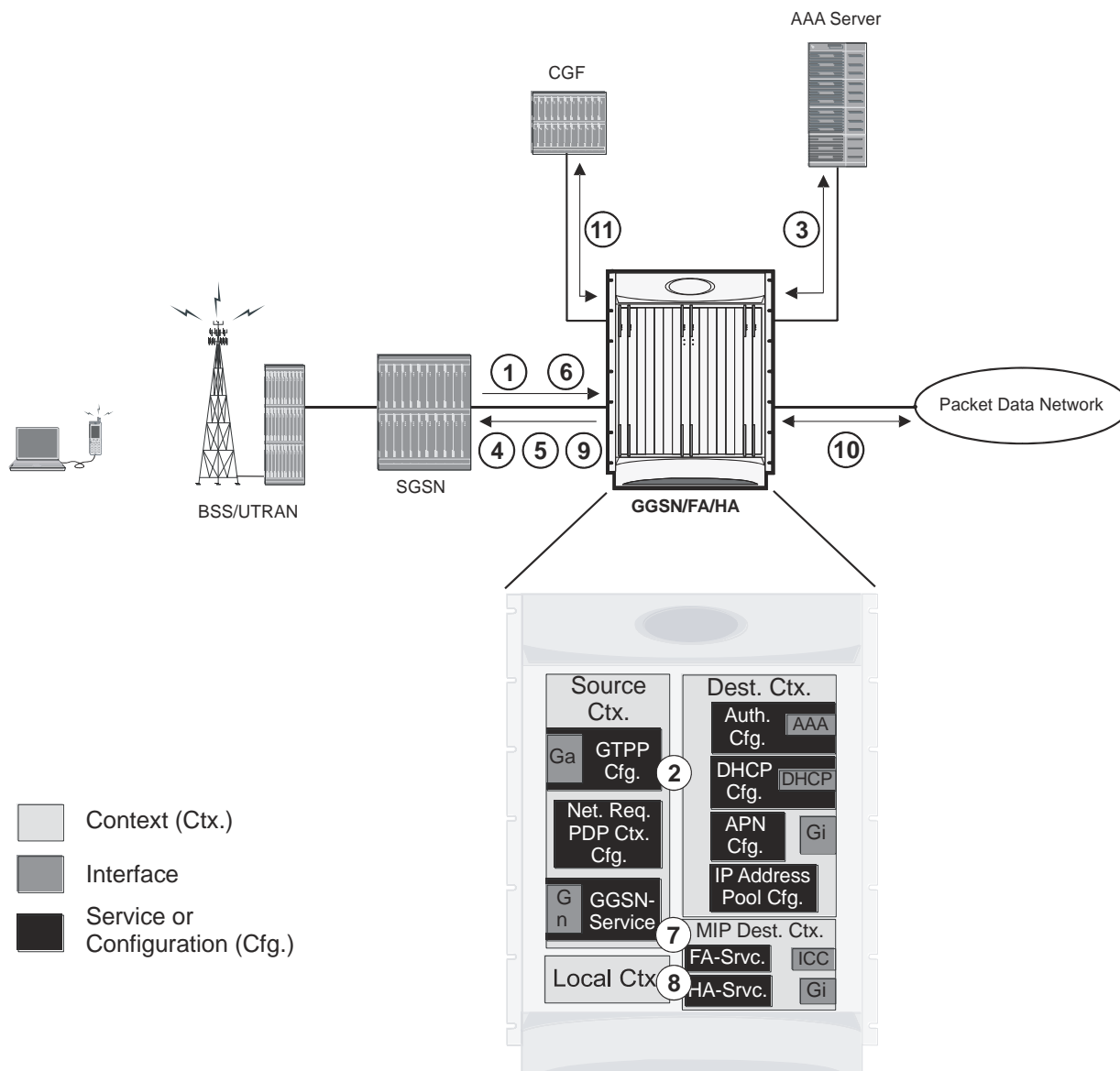
Required Information	Description
	<p><b>Replay-protection process:</b> Specifies how protection against replay-attacks is implemented. The possible processes are nonce and timestamp. The default is timestamp with a tolerance of 60 seconds.</p> <p>A replay-protection process is required for each mobile node-to-HA SPI configured.</p>
Maximum registration lifetime	<p>Specifies the longest registration lifetime that the HA service will allow in any Registration Request message from the mobile node.</p> <p>The time is measured in seconds and can be configured to any integer value between 1 and 65535. An infinite registration lifetime can also be configured by disabling the timer. The default is 600.</p>
Maximum number of simultaneous bindings	<p>Specifies the maximum number of “care-of” addresses that can simultaneously be bound for the same user as identified by NAI and Home address.</p> <p>The number can be configured to any integer value between 1 and 5. The default is 3.</p>
Default Subscriber Configuration	
“Default” subscriber’s IP context name	<p>Specifies the name of the egress context on the system that facilitates the Gi interfaces.</p> <p><b>NOTE:</b> For this configuration, the IP context name should be identical to the name of the destination context.</p>

## How This Configuration Works

This system configuration supports typical GGSN and Mobile IP functionality.

System operation for typical GGSN functionality behaves as described in *GGSN Configuration Example* chapter of this guide for each of the various call types. This section focusses on how this system configuration functions to process a Mobile IP session. The following figure and the text that follows describe how this configuration works to process calls

Figure 33. Call Processing When Using the System as a GGSN, FA, and HA



1. A Create PDP Context Request message for a subscriber session is sent from the SGSN to the GGSN service over the Gn interface. The message contains information such as the PDP Type, APN, and charging characteristics.
2. The GGSN determines whether or not it is configured with an APN identical to the one specified in the message. If so, it determines how to process the session based on the configuration of the APN. In this case, it is determined that Mobile IP must be used. From the APM configuration, the system also determines the context in which the FA service is configured.
3. If subscriber authentication is required, the GGSN authenticates the subscriber by communicating with a RADIUS server over the AAA interface.
4. The GGSN returns an affirmative Create PDP Context Response to the SGSN over the Gn interface. The home address assigned to the mobile as part of the response is 0.0.0.0 indicating that it will be reset with a Home address after the PDP context activation procedure.

5. The FA component of the GGSN sends a Agent Advertisement message to the MS. The message contains the FA parameters needed by the mobile such as one or more care-of addresses. The message is sent as an IP limited broadcast message (i.e. destination address 255.255.255.255), however only on the requesting MS's TEID to avoid broadcast over the radio interface.
6. The MS sends a Mobile IP Registration request to the GGSN/FA. This message includes either the MS's static home address or it can request a temporary address by sending 0.0.0.0 as its home address. Additionally, the request must always include the Network Access Identifier (NAI) in a Mobile-Node-NAI Extension.
7. The FA forwards the registration request from the MS to the HA while the MS's home address or NAI and TEID are stored by the GGSN. The FA service communicates with the required HA service configured in the same context over the ICC interface. In response the HA sends a registration response to the FA containing the address assigned to the MS.
8. The FA extracts the home address assigned to the MS by the HA from the response and the GGSN updates the associated PDP context. The FA then forwards it to the MS (identified by either the home address or the NAI and TEID).
9. The GGSN issues a PDP context modification procedure to the SGSN in order to update the PDP address for the MS.
10. The MS sends/receives data to/from the packet data network over the GGSN's PDN interface.
11. Upon termination of the subscriber session, the GGSN sends GGSN charging detail records to the CGF using GTPP over the Ga interface.

# Chapter 6

## GGSN Service Configuration Procedures

---


This chapter is meant to be used in conjunction with the previous chapter that describes the information needed to configure the system to support GGSN functionality for use in GPRS/UMTS networks.

It is recommended that you identify the options from the previous chapters that are required for your specific deployment. You can then use the procedures in this chapter to configure those options.


Procedures are provided for the following tasks:

- [GGSN Service Configuration](#)
- [GTPP Accounting Support Configuration](#)
- [APN Configuration](#)
- [DHCP Service Configuration](#)
- [IP Address Pool Configuration on the System](#)
- [Gn-Gp Handoff Support Configuration](#)
- [FA Services Configuration](#)
- [Common Gateway Access Support Configuration](#)
- [Rf Interface Configuration for Offline Charging](#)

---

 **Important:** At least one Packet Accelerator Card (PAC) or Packet Services Card (PSC) must be made active prior to service configuration. Information and instructions for configuring PACs/PSCs to be active can be found in the *Configuring System Settings* chapter of the *System Administration Guide*.

---

 **Caution:** While configuring any base-service or enhanced feature, it is highly recommended to take care of conflicting or blocked IP addresses and port numbers for binding or assigning. In association with some service steering or access control features, like *Access Control List* configuration, use of inappropriate port number may result in communication loss. Refer respective feature configuration document carefully before assigning any port number or IP address for communication with internal or external network.

---

# GGSN Service Configuration

GGSN services are configured within contexts and allow the system to function as a GGSN in either a GPRS or UMTS wireless data network.



**Important:** This section provides the minimum instruction set for configuring a GGSN service that allows the system to process PDP contexts. Commands that configure additional GGSN service properties are provided in the *GGSN Service Configuration Mode Commands* chapter of *Command Line Interface Reference*.

These instructions assume that you have already configured the system level configuration as described in *System Administration Guide*.

To configure the system to work as GGSN service:

- Step 1** Create the GGSN service, local User Datagram Protocol (UDP) port for the Gn interfaces' IP socket, and bind it to an IP address by applying the example configuration in the *GGSN Service Creation and Binding* section.
- Step 2** Associate the accounting context for the GGSN service and configure charging characteristic profile parameters for GGSN service by applying the example configuration in the *Accounting Context and Charging Characteristics Configuration* section.
- Step 3** Configure the SGSN and PLMN related policy and session setup timeout for the GGSN service by applying the example configuration in the *SGSN and PLMN Policy Configuration* section.
- Step 4** Optional. Configure the GGSN service to support network-requested PDP contexts by applying the example configuration in the *Network-requested PDP Context Support Configuration* section.
- Step 5** Verify your GGSN configuration by following the steps in the *GGSN Configuration Verification* section.
- Step 6** Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

## GGSN Service Creation and Binding

Use the following example to create the GGSN service and bind it to an IP address:

```
configure

    context <vpn_ctxt_name> -noconfirm

        ggsn-service <ggsn_svc_name>

    end
```

Notes:

- A maximum of 256 services (regardless of type) can be configured per system.
- Bind address should not conflict with any other GTP-based service.

## Accounting Context and Charging Characteristics Configuration

Use the following example to configure a GTPP accounting context and charging characteristics parameters for GGSN service.

```
configure

  context <vpn_ctxt_name>

    ggsn-service <ggsn_svc_name>

      accounting context <aaa_ctxt_name>

      cc profile <cc_prof_index>

    end
```

Notes:

- Charging characteristics behavior and profile index can be configured for multiple CC profile indexes. For more options and keywords like **buckets**, **interval**, **sgsns**, **tariff**, **volume** etc., refer cc profile section in Command Line Interface Reference.
- This command works in conjunction with the **cc-sgsn** command located in the APN configuration mode that dictates which CCs should be used for subscriber PDP contexts. Refer to the *APN Configuration* section in this chapter.

## SGSN and PLMN Policy Configuration

Use the following example to configure the SGSN and PLMN related policy and session setup timeout for the GGSN service:

```
configure

  context <vpn_ctxt_name>

    ggsn-service <ggsn_svc_name>

      plmn id mcc <mcc_number> mnc <mnc_number> [primary]

      sgsn address <ip_address> / <subnet_mask>

      plmn unlisted-sgsn [foreign | home | reject]

      setup-timeout <dur_sec>

    end
```

Notes:

- SGSN or PLMN related policy can be defined for multiple SGSNs or PLMN.
- For optional configuration parameters of SGSN address, refer Command Line Interface Reference.



**Important:** The GGSN only communicates with the SGSNs configured using this command unless a PLMN policy is enabled to allow communication with unconfigured SGSNs. PLMN policies are configured using the **plmn unlisted-ggsn** command.

## Network-requested PDP Context Support Configuration

Use the following example to configure the GGSN to support the network-requested PDP context:

```
configure

    context <vpn_ctxt_name>

        network-requested-pdp-context activate <ip_address> dst-context <dst_ctxt_name>
    imsi <imsi> apn <apn_name>

        network-requested-pdp-context gsn-map <ip_address>

    end
```

Notes:

- It is recommended that this functionality be configured in the system source context(s) along with the GGSN service(s).
- Up to 1000 IP address can be configured for network request PDP context support.
- Only one GSN-MAP node can be configured per system context.

## GGSN Configuration Verification

**Step 1** Verify that your GGSN services were created and configured properly by entering the following command in Exec Mode:

```
show ggsn-service name <ggsn_svc_name>}
```

The output of this command given below is a concise listing of GGSN service parameter settings as shown in the sample output displayed. In this example, a GGSN service called *ggsn1* was configured and you can observe some parameters configured as default.

```
Service name:                ggsn1
Context:                     ggsn1
Associated PGW svc:          None
Associated GTPU svc:          None
Accounting Context Name:     ggsn1
dns-client Context Name:
Authorize:                    Disabled
```



```
Fqdn-name:                Disabled

Bind:                      Done

Local IP Address:          192.168.70.1          Local IP Port: 2123

Self PLMN Id.:            MCC: 450, MNC: 06

Retransmission Timeout:   20 (secs)

Max Retransmissions:      4

Restart Counter:          16

Echo Interval:             60 (secs)

Guard Interval:           100 (secs)

Setup Timeout:            60 (secs)

PLMN Policy:              Reject unlisted SGSN

Reject Code Policy:

    Authentication Server Timeout: User Authentication Failed

    Accounting Server Timeout:    No Resources Available

Ran Procedure Ready:      Disabled

NSAPI in Create PDP response: Disabled

Duplicate Subscriber Addr Request: Reject

trace-collection-entity: Disabled

Path Failure Detection on gtp msgs: Echo

GTP Private Extensions:

    None

Max IP sessions:          4000000

Max PPP sessions:         2500000

Max sessions:             4000000

Service Status:           Started

Newcall Policy:           None

MBMS Policy:              None

MBMS Charging ID Optimization: Disabled

3GPP Qos to DSCP Mapping (for G-PDUs):
```

```

qci 1:      ef
qci 2:      ef
qci 3:      af11
qci 4:      af11
qci 5:      ef
qci 6:      ef
qci 7:      af21
qci 8:      af21
qci 9:      be

```

3GPP Qos to DSCP Mapping based on Alloc. Prio:

```

qci 5 (Alloc. P 1):  ef
qci 5 (Alloc. P 2):  ef
qci 5 (Alloc. P 3):  ef
qci 6 (Alloc. P 1):  ef
qci 6 (Alloc. P 2):  ef
qci 6 (Alloc. P 3):  ef
qci 7 (Alloc. P 1):  af21
qci 7 (Alloc. P 2):  af21
qci 7 (Alloc. P 3):  af21
qci 8 (Alloc. P 1):  af21
qci 8 (Alloc. P 2):  af21
qci 8 (Alloc. P 3):  af21
GTPC messages:      be
Background:          be

```

Charging Characteristics(CC) Behaviors:

```
No records (Bit No.):  0
```

Charging Characteristics(CC) Profiles:

```
Profile 0:
```

```
Buckets: 4
```

```
SGSN changes: 4
```

Profile 1:

Buckets: 4

SGSN changes: 4

SGSN Configuration List:

sgsn address 2.2.2.2/32 mcc 111 mnc 999 description aaa-ggsn

**Step 2** Verify configuration for errors by entering the following command in Exec Mode:

**show configuration errors section ggsn-service verbose**

# GTPP Accounting Support Configuration

This section provides instructions for configuring GTPP-based accounting for subscriber PDP contexts. GTPP-based accounting for a subscriber can be configured by CGF server configuration in a GTPP group. Additionally individual CGF server can be configured with this example.



**Important:** To configure RADIUS and Diameter AAA functionality, refer *AAA Interface Administration and Reference*.

When the GTPP protocol is used, accounting messages are sent to the charging gateways (CGs) over the Ga interface. The Ga interface and GTPP functionality are typically configured within the system's source context. CDRs are generated according to the interim triggers configured using the charging characteristics configured for the GGSN, and a CDR is generated when the session ends.

GTPP version 2 is used by default. However, if version 2 is not supported by the CGF, the system reverts to using GTPP version 1. All subsequent CDRs are always fully-qualified partial CDRs. For CDR encoding different dictionaries are supported. For more information on GTPP dictionaries, refer *AAA Interface Administration and Reference*.

Whether or not the GGSN accepts charging characteristics from the SGSN can be configured on a per-APN basis based on whether the subscriber is visiting, roaming or, home.

By default, the GGSN always accepts the charging characteristics from the SGSN. However it accepts charging characteristics from RADIUS too, they must always be provided by the SGSN for GTPPv1 requests for primary and secondary PDP contexts.

If the system is configured to reject the charging characteristics from the SGSN, the GGSN can be configured with its own that can be applied based on the subscriber type (visiting, roaming, or home) at the APN level (refer to the *APN Configuration* section of this chapter for more information). GGSN charging characteristics consist of a profile index and behavior settings (refer to the *GGSN Service Configuration* section of this chapter for more information). The profile indexes specify the criteria for closing accounting records based specific criteria (refer to the *GGSN Service Configuration* section of this chapter for more information).



**Important:** This section provides the minimum instruction set for configuring a GTPP accounting support in a GGSN service. Commands that configure additional GTPP accounting properties are provided in the *Command Line Interface Reference* guide.

These instructions assume that you have already configured the system level configuration as described in *System Administration Guide* and GGSN service as described in *GGSN Service Configuration* section of this chapter.

To configure the GTPP accounting support for a GGSN service:

- Step 1** Create the GTPP group in accounting context by applying the example configuration in the *GTPP Group Creation* section.
- Step 2** Configure the charging agent and GTPP server (CGF) related parameters for the GTPP accounting support by applying the example configuration in the *GTPP Group Configuration* section.
- Step 3** Verify your GTPP group and accounting configuration by following the steps in the *GTPP Group Configuration Verification* section.
- Step 4** Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

## GTPP Group Creation

Use the following example to create the GTPP group to support GTPP accounting:

```
configure

    context <vpn_ctxt_name>

        gtpv group <gtpv_group_name> -noconfirm

    end
```

Notes:

- In addition to one default GTPP group “default” a maximum of 8 GTPP groups can be configured with this command in a context.
- In case no GTPP group is configured in this context, system creates a default GTPP group named “default” and all the CGF servers and their parameters configured in this context are applicable to this “default” GTPP group.

## GTPP Group Configuration

Use the following example to configure the GTPP server parameters, GTPP dictionary, and optionally CGF to support GTPP accounting:

```
configure

    context <vpn_ctxt_name>

        gtpv group <gtpv_group_name>

            gtpv charging-agent address <ip_address> [port <port>]

            gtpv server <ip_address> [max <msgs >] [priority <priority>]

            gtpv dictionary <dictionaries>

            gtpv max-cdrs <number_cdrs> [wait-time <dur_sec>]

            gtpv transport-layer {tcp | udp}

        end
```

Notes:

- In addition to one default GTPP group “default” a maximum of 8 GTPP groups can be configured with this command in a context.
- In case no GTPP group is configured in this context, system creates a default GTPP group named “default” and all the CGF servers and their parameters configured in this context are applicable to this “default” GTPP group.
- Command for CGF **gtpv charging-agent** is optional and configuring gtpv charging-agent on port 3386 may interfere with ggsn-service configured with the same ip address. Multiple interfaces can be configured within a single context if needed.

- For more information on GTPP dictionary encoding in addition to referring Command Line Interface Reference, refer AAA Interface Administration and Reference.
- For better performance, it is recommended to configure maximum number of CDRs as 255 with **gtp max-cdrs** command.
- Operator can select transport layer protocol as TCP or UDP for Ga interface with **gtp transport-layer** command.
- Multiple GTPP server can be configured using multiple instances of this command subject to following limits:
  - Total 4 GTPP server in one GTPP group
  - Total 32 GTPP server in one context or in the overall configuration
  - Total 33 GTPP groups (1 default and 32 user defined GTPP groups) can be configured in one context. Number of CGFs in 1 GTPP group is limited to 4 and a total of 32 CGF servers across all GTPP groups in one context are configurable.
  - Total 32 GTPP groups can also be configured under an APN

## GTPP Group Configuration Verification

**Step 1** Verify that your CGFs were configured properly by entering the following command in Exec Mode:

```
show gtp accounting servers
```

This command produces an output similar to that displayed below:

```
context: source

Preference IP          Port  Priority  State      Group
-----
Primary  192.168.32.135    3386    1        Active    default
Primary  192.168.89.9      3386   100        Active    default
```

**Step 2** Verify configuration for errors by entering the following command in Exec Mode:

```
show configuration errors section ggsn-service verbose
```

# APN Configuration

This section provides instructions for configuring the APN templates that are used to determine how PDP contexts should be processed. APNs are configured in system authentication contexts.



**Important:** This section provides the minimum instruction set for configuring APNs in a GGSN service. Commands that configure additional APN properties are provided in *APN Configuration Mode Commands* chapter of *Command Line Interface Reference*.

These instructions assume that you have already configured the system level configuration as described in System Administration Guide and GGSN service as described in the *GGSN Service Configuration* section of this guide.

To configure the APN properties for a GGSN service:

- Step 1** Create the APN in system context and specify the support of PDP contexts and selection mode by applying the example configuration in the APN Creation and Configuration section.
- Step 2** Configure the authentication and accounting parameters in APN by applying the example configuration in the Authentication, Accounting, and GTPP Group Configuration in APN section.
- Step 3** Configure the IP allocation method in APN by applying the example configuration in the IP Address Allocation Method Configuration in APN section.
- Step 4** Optional. Configure the charging characteristics related parameters for the APN by applying the example configuration in the Charging Characteristics Parameter Configuration in APN section.
- Step 5** Optional. Configure virtual APNs by applying the example configuration in the Virtual APN Configuration section.
- Step 6** Optional. Configure other optional parameters for the APN by applying the example configuration in the Other Optional Parameter Configuration in APN section.
- Step 7** Verify your APN configuration by following the steps in the APN Configuration Verification section.
- Step 8** Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

## APN Creation and Configuration

Use the following example to create and configure the APNs:

```
configure

context <vpn_ctxt_name>

  apn <apn_name> -noconfirm

  max-contexts primary <number> total <total_number>

  pdp-type {ipv4 [ipv6] | ipv6 [ipv4] | ppp}

  selection-mode {sent-by-ms | chosen-by-sgsn | subscribed}
```

```
ip context-name <dst_ctxt_name>

end
```

Notes:

- Up to 1000 APNs can be configured on a system.
- APN templates should be created/configured within system authentication contexts or destination context.
- Selection mode parameter's setting must be identical to the selection mode setting on the SGSN(s) that the GGSN communicates with. The GGSN rejects attempts to establish PDP contexts from any SGSN having a different setting.
- For IPv6 calls to work, the destination context must have an IPv6 interface configured in it.
- If the APN supports Mobile IP for subscriber PDP contexts, then ip context-name command is used to indicate the context in which the FA service is configured.
  - If no context name is specified, the system uses the context in which the APN is configured.
  - If Mobile IP is supported and no name is specified, the system uses the context in which the GGSN service facilitating the PDP context is located.

## Authentication, Accounting, and GTPP Group Configuration in APN

This section describes the procedure to configure the authentication and accounting parameters for an APN. It also specify the procedure to attach a GTPP group with an APN.

- Step 1** Configure the authentication and accounting parameters by applying the example configuration in the *Authentication and Accounting Configuration in APN* section.
- Step 2** Attach a GTPP group with APN by applying the example configuration in the *GTPP Group Association to APN* section.

### Authentication and Accounting Configuration in APN

Use the following example to configure the accounting mode and authentication parameter for APN:

```
configure

context <dst_ctxt_name>

  apn <apn_name>

    accounting-mode {none | gtp | radius [no-interims] [no-early-pdus]}

    default authentication

  end
```

Notes:

- APNs are configured in system authentication contexts or destination context.
- The authentication process varies depending on whether the PDP context is of type IP or PPP. The **authentication** command provides **imsi-auth**, **msisdn-auth**, **eap initial-access-request**,



**allow-noauth**, **chap**, **mschap**, and **pap** options. For more information on type of authentication, refer authentication section in APN Configuration Mode Commands chapter of Command Line Interface Reference.

## GTPP Group Association to APN

After configuring GTPP group at context-level, an APN within the same context can be configured to use the user defined GTPP group.

Refer section *GTPP Accounting Support Configuration* for GTPP group configuration.

```
configure

context <vpn_ctxt_name>

  apn <apn_name>

    gtp group <gtp_group_name> [accounting-context <aaa_ctxt_name>]

  end
```


Notes:

- GTPP group must be configured before associating with APN or “default” GTPP group can be used.

## IP Address Allocation Method Configuration in APN

Use the following example to configure the IP address allocation method for APN:

---

 **Important:** Additional charging characteristics parameters are configurable as part of the GGSN service. Refer to the *GGSN Service Configuration* section of this chapter for more information.

---

```
configure

context <dst_ctxt_name>

  apn <apn_name>

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

  end
```

Notes:


- The process used by the system to determine how the address should be allocated. For detail information on IP address allocation, refer Usage section of **ip address alloc-method** command in *APN Configuration Mode Commands* chapter of Command Line Interface Reference.
- If DHCP-Proxy and DHCP-Relay method is selected for IP address allocation, a DHCP service must be configured on the system as described in *DHCP Service Configuration* section and specified the name of DHCP Service by entering the **dhcp service-name** command as described in APN Configuration Mode Commands chapter of Command Line Interface Reference.

- If local pool is selected for IP address allocation, a local pool must be configured on the system as described in *IP Address Pool Configuration on the System* section and specified the name of a private IP address pool by entering the **ip address pool** command as described in APN Configuration Mode Commands chapter of Command Line Interface Reference.

## Charging Characteristics Parameter Configuration in APN

Use the following example to configure the charging characteristics parameter for APN:

---

 **Important:** Additional charging characteristics parameters are configurable as part of the GGSN service. Refer to the *GGSN Service Configuration* section of this chapter for more information.

---

```
configure

context <dst_ctxt_name>

    apn <apn_name>

        cc-sgsn {home-subscriber-use-GGSN | roaming-subscriber-use-GGSN | visiting-
subscriber-use-GGSN}+

            cc-home behavior <bit> profile <index>

            cc-roaming behavior <bit> profile <index>

            cc-visiting behavior <bit> profile <index>

        end
```

Notes:

- If multiple behavior bits are configured for a single profile index, the variable bits is achieved by “Or”ing the bit strings and converting the result to hexadecimal.

### Example

If behavior bits 5 (0000 0001 0000) and 11 (0100 0000 0000) are both being assigned to profile index 5 for a home subscriber, the appropriate command is **cc-home behavior 410 profile 5**.

## Virtual APN Configuration

Virtual APNs are references (or links) to alternative APNs to be used for PDP context processing based on properties of the context. Use the following example to configure the virtual APNs.

```
configure

context <dst_ctxt_name>

    apn <apn_name>

        virtual-apn preference <priority> apn <apn_name> { access-gw-address <IP_addr |
IP_addr/mask> | bearer-access-service <bearer_access_svc_name> | cc-profile
<cc_profile_index> | domain <domain_name> | mcc <mcc_number> mnc <mnc_number> | msisdn-
```

```

range from <start_range> to <end_range> | rat-type { eutran | gan | geran | hspa | utran
| wlan } | roaming-mode { home | visiting | roaming }

end

```

Notes:

- Up to 1023 references can be configured per APN. Additional information about “virtual” APNs and their operation can be found in the *Command Line Interface Reference*.

## Other Optional Parameter Configuration in APN

Use the following example to configure various optional parameter for APN:

```

configure

context <dst_ctxt_name>

  apn <apn_name>

    dns {primary | secondary} {<dns_ip_address>}

    mobile-ip required

    mobile-ip home-agent <ha_ip_address>

    ip source-violation {ignore | check [drop-limit <limit>]} [exclude-from-
accounting]

    restriction-value <value>

    timeout {absolute | idle | qos-renegotiate} <timeout_dur>

    timeout long-duration <ldt_dur> [inactivity-time <inact_dur>]

    long-duration-action detection

    long-duration-action disconnection [suppress-notification] [dormant-only] +

end

```

Notes:

- Mobile is supported for IP PDP contexts only. Mobile IP configuration attributes returned as part of a successful authentication during the GTP authentication phase (for non-transparent IP PDP contexts) supersede the APN configuration. Any attributes returned during the FA authentication phase are ignored.
- If mobile-ip required option is enabled, the system deletes any PDP context using the APN that can not establish a Mobile IP session.

## APN Configuration Verification

**Step 1** Verify that your APN were configured properly by entering the following command in Exec Mode:

**show apn all**

This command produces an output similar to that displayed below is an excerpt from a sample output. In this example, an APN called *apn1* was configured.

```

access point name (APN):  apn1
authentication context:    test

pdp type:  ipv4

ehrpd access:  N/A

Selection Mode:  subscribed

ip source violation:  Checked                drop limit:  10

accounting mode: gtpv6                        No early PDUs: Disabled

no-interims:  Disabled

Bearer Control Mode:  none

max-primary-pdp-contexts:  1000000          total-pdp-contexts:  1000000
current primary-pdp-contexts:  0            total-pdp-contexts:  0
primary contexts:  not available            total contexts: not available
max secondary contexts per-subscriber:  10  IMS Authorization:  disabled
Credit Control:  disabled

mbms bearer absolute timeout:  0            mbms bearer idle timeout:  0
mbms ue absolute timeout:  0

permission:

local ip:  0.0.0.0                          nexthop gateway addr:
primary dns:  0.0.0.0                        secondary dns:  0.0.0.0
primary nbns:  0.0.0.0                      secondary nbns:  0.0.0.0
ppp keep alive period :  0                  ppp mtu :  1500
absolute timeout :  0                      idle timeout :  0
idle-timeout-activity ignore-downlink:  Disabled
long duration timeout:  0                  long dur inactivity
time:  Disabled

long duration action:  Detection

wimax header compression/suppression:  none

```

```

ip header compression:  vj
ip hide service address:  Disabled
ip output access-group:                                     ip input access-group:
ipv6 output access-group:                                   ipv6 input access-group:
policy-group in:                                           policy-group out:
permit ip multicast:  False
ppp authentication:
eap authentication initial-access-request:  authenticate-authorize
allow noauthentication:  Enabled                imsi authentication:  Disabled
msisdn authentication:  Disabled
ip destination context:  ip-ctx
Rule Base:  default
FW-and-NAT Policy:  default
Bandwidth-Policy:  default
Link-Monitoring:  OFF
Content-Filtering Policy-Id:  Not configured
mediation accounting:  Disabled
mediation-device context:  Not set                mediation no early
PDUs:  Disabled
mediation no-interims:  Disabled                mediation delay-GTP-response:
Disabled
outbound username:  N/A
ip address pools:  N/A
ip address secondary pools:  N/A
access-link ip-frag:  df-ignore
ignore DF-bit data-tunnel:  On
ip allocation type:  local pool                allow user specified ip addr:
true
prefer dhcp options:  false
allow deferred:  true

```

## 3GPP Qos to DSCP Mapping:

```

qci 1:      ef
qci 2:      ef
qci 3:      af11
qci 4:      af11
qci 5:      ef
qci 6:      ef
qci 7:      af21
qci 8:      af21
qci 9:      be

```

## 3GPP Qos to DSCP Mapping based on Alloc. Prio:

```

qci 5 (Alloc. P 1):  ef
qci 5 (Alloc. P 2):  ef
qci 5 (Alloc. P 3):  ef
qci 6 (Alloc. P 1):  ef
qci 6 (Alloc. P 2):  ef
qci 6 (Alloc. P 3):  ef
qci 7 (Alloc. P 1):  af21
qci 7 (Alloc. P 2):  af21
qci 7 (Alloc. P 3):  af21
qci 8 (Alloc. P 1):  af21
qci 8 (Alloc. P 2):  af21
qci 8 (Alloc. P 3):  af21

```

GTPP Group: gtpg-gp            GTPP Accounting Context: acc

Mobile IPv6 Tunnel MTU: 1500

Mobile IPv6 Tunnel MTU Exceed Action: notify-sender

Mobile IPv6 Home Agent: none

Mobile IPv6 Home Link Prefix: ::/0

Mobile IPv6 Home Address: none

**Step 2** Verify configuration for errors in APN configuration by entering the following command in Exec Mode:

```
show configuration errors section ggsn-service verbose
```

## DHCP Service Configuration

The system can be configured to use the Dynamic Host Control Protocol (DHCP) to assign IP addresses for PDP contexts. IP address assignment using DHCP is done using one of two methods as configured within an APN:

- **DHCP-proxy:** The system acts as a proxy for client (MS) and initiates the DHCP Discovery Request on behalf of client (MS). Once it receives an allocated IP address from DHCP server in response to DHCP Discovery Request, it assigns the received IP address to the MS. This allocated address must be matched with the an address configured in an IP address pool on the system. This complete procedure is not visible to MS.

As the number of addresses in memory decreases, the system solicits additional addresses from the DHCP server. If the number of addresses stored in memory rises above the configured limit, they are released back to the DHCP server.

- **DHCP-relay:** The system acts as a relay for client (MS) and forwards the DHCP Discovery Request received from client (MS). Once it receives an allocated IP address from DHCP server in response to DHCP Discovery Request, it assigns the received IP address to the MS.

Regardless of the DHCP method, there are parameters that must first be configured that specify the DHCP servers to communicate with and how the IP address are handled. These parameters are configured as part of a DHCP service.



**Important:** This section provides the minimum instruction set for configuring a DHCP service on system for DHCP-based IP allocation. For more information on commands that configure additional DHCP server parameters and working of these commands, refer DHCP Service Configuration Mode Commands chapter of Command Line Interface Reference.

These instructions assume that you have already configured the system level configuration as described in *System Administration Guide* and GGSN service as described in *GGSN Service Configuration* section of this chapter.

To configure the DHCP service:

- Step 1** Create the DHCP service in system context and bind it by applying the example configuration in the *DHCP Service Creation* section.
- Step 2** Configure the DHCP servers and minimum and maximum allowable lease times that are accepted in responses from DHCP servers by applying the example configuration in the *DHCP Server Parameter Configuration* section.
- Step 3** Verify your DHCP Service configuration by following the steps in the *DHCP Service Configuration Verification* section.
- Step 4** Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

## DHCP Service Creation

Use the following example to create the DHCP service to support DHCP-based address assignment:

```
configure
    context <dest_ctxt_name>
        dhcp-service <dhcp_svc_name>
```



```

        bind address <ip_address> [nexthop-forwarding-address <nexthop_ip_address>
[mppls-label input <in_mpls_label_value> output <out_mpls_label_value1>
[out_mpls_label_value2]]]

    end

```

Notes:

- To ensure proper operation, DHCP functionality should be configured within a destination context.
- Optional keyword **nexthop-forwarding-address** <nexthop\_ip\_address> [**mppls-label input** <in\_mpls\_label\_value> **output** <out\_mpls\_label\_value1> [ out\_mpls\_label\_value2 ]] applies DHCP over MPLS traffic.

## DHCP Server Parameter Configuration

Use the following example to configure the DHCP server parameters to support DHCP-based address assignment:

configure

```

context <dest_ctxt_name>

    dhcp-service <dhcp_svc_name>

        dhcp server <ip_address> [priority <priority>

        dhcp server selection-algorithm {first-server | round-robin}

        lease-duration min <minimum_dur> max <max_dur>

        dhcp deadtime <max_time>

        dhcp detect-dead-server consecutive-failures <max_number>

        max-retransmissions <max_number>

        retransmission-timeout <dur_sec>

    end

```

Notes:

- Multiple DHCP can be configured by entering **dhcp server** command multiple times. A maximum of 20 DHCP servers can be configured.
- The **dhcp detect-dead-server** command and **max-retransmissions** command work in conjunction with each other.
- The retransmission-timeout command works in conjunction with **max-retransmissions** command.

## DHCP Service Configuration Verification

**Step 1** Verify that your DHCP servers configured properly by entering the following command in Exec Mode:

```
show dhcp service all
```

This command produces an output similar to that displayed below where DHCP name is *dhcp1*:

```

Service name:                dhcp1

Context:                     isp

Bind:                        Done

Local IP Address:            150.150.150.150

Next Hop Address:            192.179.91.3

    MPLS-label:

        Input:                5000

        Output:               1566  1899

Service Status:              Started

Retransmission Timeout:      3000 (milli-secs)

Max Retransmissions:         2

Lease Time:                   600 (secs)

Minimum Lease Duration:       600 (secs)

Maximum Lease Duration:       86400 (secs)

DHCP Dead Time:              120 (secs)

DHCP Dead consecutive Failure:5

DHCP T1 Threshold Timer:     50

DHCP T2 Threshold Timer:     88

DHCP Client Identifier:       Not Used

DHCP Algorithm:              Round Robin

DHCP Servers configured:

    Address: 150.150.150.150    Priority: 1

DHCP server rapid-commit: disabled

DHCP client rapid-commit: disabled

DHCP chaddr validation: enabled

```

**Step 2** Verify the DHCP service status by entering the following command in Exec Mode:

```
show dhcp service status
```

## IP Address Pool Configuration on the System

Before an MS is able to access data services, they must have an IP address. As described previously, the GGSN supports static or dynamic addressing (through locally configured address pools on the system, DHCP client-mode, or DHCP relay-mode). Regardless of the allocation method, a corresponding address pool must be configured.


IP addresses can be dynamically assigned from a single pool/a group of IP pools/a group of IP pool groups. The addresses/IP pools/ IP pool groups are placed into a queue in each pool or pool group. An address is assigned from the head of the queue and, when released, returned to the end. This method is known as least recently used (LRU).


On initiation of a session, a request of IP address from IP pool is sent and system assigns an IP address out of "available" IP address(es) in the pool. This assigned IP address is set to "allocated" state and cannot be used for any other session during this state. As soon as the session is cleared the state of "allocated" IP address is changed to "released" and is ready for allocation to any other subscriber session. If a "hold" timer is set for assigned/released IP address(es), it will go into the "hold" state and remain there till the timer expires. As soon as "hold timer" expires its state is changed from "hold" to "released" state and it will be available for reallocation. The "available" IPs include "free" and "released" IP addresses.

Free IPs are used first depending on which subscriber is connecting. Normally same IP is given to a subscriber. So if a subscriber is connecting again, instead of using a free IP, GGSN allocates the IP which was given to him previously. This IP will be from the released state. For GGSN, Username and IMSI are used as key for generating subscriber ID used by VPN while allocating IP from the IP pool. Therefore if the subscriber ID matches to any of the previous ones for IPs in released state, that IP is re-allocated to that subscriber, otherwise a new IP is allocated.

When a group of pools have the same priority, an algorithm is used to determine a probability for each pool based on the number of available addresses, then a pool is chosen based on the probability. This method, over time, allocates addresses evenly from the group of pools.

---

 **Important:** Setting different priorities on each individual pool can cause addresses in some pools to be used more frequently.

 **Important:** This section provides the minimum instruction set for configuring local IP address pools on the system. For more information on commands that configure additional parameters and options, refer *ip pool* command section in *Context Configuration Mode Commands* chapter of *Command Line Interface Reference*.

---

These instructions assume that you have already configured the system level configuration as described in *System Administration Guide* and GGSN service as described in *GGSN Service Configuration* section of this chapter.

To configure the IP pool:

- Step 1** Create the IP pool for IPv4 addresses in system context by applying the example configuration in the *IPv4 Pool Creation* section.
- Step 2** Optional. Configure the IP pool for IPv6 addresses in system context by applying the example configuration in the *IPv6 Pool Creation* section.
- Step 3** Verify your IP pool configuration by following the steps in the *IP Pool Configuration Verification* section.
- Step 4** Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

## IPv4 Pool Creation

Use the following example to create the IPv4 address pool:

```
configure

    context <dest_ctxt_name>

        ip pool <pool_name> <ip_address/mask> [{private| public}[priority]] | static

    end
```

Notes:

- To ensure proper operation, IP pools should be configured within a destination context.
- Each address in the pool requires approximately 24 bytes of memory. Therefore, in order to conserve available memory, the number of pools may need to be limited depending on the number of addresses to be configured and the number of PACs/PSCs installed.
- Setting different priorities on individual pools can cause addresses in some pools to be used more frequently.
- For more information on commands/keywords that configure additional parameters and options, refer `ipv6 pool` command section in Context Configuration Mode Commands chapter of Command Line Interface Reference.

## IPv6 Pool Creation

Use the following example to create the IPv6 address pool:

```
configure

    context <dest_ctxt_name>

        ipv6 pool <pool_name> 6to4 local-endpoint
        <ip_address>[private][public][shared][static]

    end
```

Notes:

- To ensure proper operation, IP pools should be configured within a destination context.
- Each address in the pool requires approximately 24 bytes of memory. Therefore, in order to conserve available memory, the number of pools may need to be limited depending on the number of addresses to be configured and the number of PACs/PSCs installed.
- Setting different priorities on individual pools can cause addresses in some pools to be used more frequently.
- For more information on commands/keywords that configure additional parameters and options, refer `ipv6 pool` command section in Context Configuration Mode Commands chapter of Command Line Interface Reference.

## IP Pool Configuration Verification

**Step 1** Verify that your IPv4 address pool configured properly by entering the following command in Exec Mode:

```
show ip pool
```

The output from this command should look similar to the sample shown below. In this example all IP pools were configured in the *isp1* context.

```
context : isp1:

+-----Type:      (P) - Public      (R) - Private
|
|                (S) - Static      (E) - Resource
|
|+-----State:    (G) - Good        (D) - Pending Delete      (R)-Resizing
||
||+---Priority: 0..10 (Highest (0) .. Lowest (10))
||||
||||+---Busypool: (B) - Busypool configured
|||||
|||||

vvvvv Pool Name   Start Address      Mask/End Address      Used      Avail
-----
PG00 ipsec        12.12.12.0           255.255.255.0         0          254
RG00 pool3        30.30.0.0            255.255.0.0           0          65534
SG00 pool2        20.20.0.0            255.255.0.0           10         65524
PG00 pool1        10.10.0.0            255.255.0.0           0          65534
SG00 vpnpool      192.168.1.250        192.168.1.254         0          5

Total Pool Count: 5
```

**Step 2** Verify that your IPv6 address pools configured properly by entering the following command in Exec Mode:

```
show ipv6 pools
```

The output from this command should look similar to the sample shown above except IPv6 addresses.

## Gn-Gp Handoff Support Configuration

This section describes all about the configurations that are required to enable the handoff between the 3GPP 2G/3G SGSN and P-GW over Gn-Gp interfaces.



**Important:** This feature is a license-enabled support and you may need to install a feature specific session license on your system to use some commands related to this configuration.

These instructions assume that you have already configured the system level configuration as described in *System Administration Guide*, GGSN service as described in *GGSN Service Configuration* section in this chapter.

To configure the Gn-Gp handoff on GGSN node:

- Step 1** Create and configure the GTP-U service by applying the example configuration in the *GTP-U Service Configuration* section.
- Step 2** Modify GGSN service to facilitate the handoff between SGSN/GGSN and P-GW by applying the example configuration in the *Modifying GGSN Configuration for Gn-Gp Handoff* section.
- Step 3** Modify APN configuration to the “subscribed” selection mode by applying the example configuration in *APN Configuration for Gn-Gp Handoff* section.
- Step 4** Verify your handoff configuration by following the steps in the *Gn-Gp Configuration Verification* section.
- Step 5** Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

## GTP-U Service Configuration

Use the following example to configure the GTP-U service:

```
configure

context <ctxt_name> -noconfirm

    gtpu-service <gtpu_svc_name>

        bind ipv4-address <ip_address>

        echo-interval <time_interval>

    end
```

Notes:

- <ctxt\_name> is name of the context which contains GTPU service on system.
- <time\_interval> is the time interval in seconds at which GPRS Tunneling Protocol (GTP) v1-U Echo packets are sent.
- <ip\_address> is the IP address of IPv4 or IPv6 type to which the GTP-U service will be binded.

## Modifying GGSN Configuration for Gn-Gp Handoff

Use the following example to create/modify the GGSN config for this feature.

```
configure

context <ctxt_name>

    ggsn-service <ggsn_svc_name>

        associate gtpu-service <gtpu_svc_name>

        associate pgw-service <pgw_svc_name>

        bind address <ip_address>

    end
```

Notes:

- <ggsn\_svc\_name> is name of the existing GGSN service.
- <gtpu\_svc\_name> is name of the existing GTP-U service created in *GTP-U Service Configuration* example.
- <pgw\_svc\_name> is the existing P-GW service name.
- <ip\_address> is the same IP address to which GTP-U service is binded in *GTP-U Service Configuration* example.
- <ctxt\_name> is the name of the context which contains the GGSN service.

## APN Configuration for Gn-Gp Handoff

Use the following example to modify the APN configuration for the smooth handover support between SGSN/GGSN and P-GW:

```
configure

context <ctxt_name>

    apn <apn_name>

        selection-mode subscribed

        ip context-name <ctxt_name>

        pdp-type <ipv4 | ipv6>

    end
```

Notes:

- Make sure that the APN Selection mode parameters setting is set to “subscribed”, which is also the default mode.

## Gn-Gp Configuration Verification

- Step 1** Verify that all the configurations made in a specific context under Context Configuration mode are in place and the P-GW service and GTP-U services have been associated to the GGSN service by entering the following command in Exec mode:

```
show ggsn-service name ggsn
```

The output from this command should look similar to the sample shown below. In this example context name *A* was created in Exec mode, GGSN service *ggsn* was created in GGSN Service Configuration mode, PGW service named *pgw* was an already configured service and GTP-U service named *gtpu* was configured in the GTPU Service Configuration mode:

```
Service name:          ggsn

context:              A

Associated PGW svc:    pgw

Associated GTPU svc:   gtpu

.

.

Bind:                 Done

Local IP Address:      120.56.45.12      Local IP Port: 2123

...

...

Echo Interval:        60 (secs)

.

.

.
```



# FA Services Configuration

FA services are configured within contexts and allow the system to function as an FA in the 3G wireless data network.

**Important:** This section provides the minimum instruction set for configuring an FA service that allows the system to process data sessions. Commands that configure additional FA service properties are provided in the Command Line Interface Reference. Additionally, when configuring Mobile IP take into account the MIP timing considerations discussed in *Mobile-IP and Proxy-MIP Timer Considerations*.

These instructions assume that you have already configured the system level configuration as described in *System Administration Guide* and GGSN service as described in *GGSN Service Configuration* section of this chapter.

To configure the FA service:

- Step 1** Create the FA service in the system context created to facilitate FA service by applying the example configuration in the *FA Service Creation* section.
- Step 2** Bind the configured FA service to a local IP address interface with UDP port and specify the maximum number of subscribers that can access this service for the Pi interfaces' IP socket by applying the example configuration in the *IP Interface and UDP Port Binding for Pi Interface* section.
- Step 3** Configure the security parameter index (SPI) between FA service and HA by applying the example configuration in the *Security Parameter Index (SPI) Configuration* section.
- Step 4** Specify the FA agent advertisement related parameters like lifetime, number of advertisements, and registration lifetime by applying the example configuration in the *FA Agent Advertisement Parameter Configuration* section.
- Step 5** Configure the number of registration per subscriber, authentication procedure, and registration timeout parameters for this FA service by applying the example configuration in the *Subscriber Registration, Authentication and Timeout Parameter Configuration* section.
- Step 6** Optional. Configure the FA service for controlling the negotiation and sending of the I-bit in revocation messages by applying the example configuration in the *Revocation Message Configuration* section.
- Step 7** Verify your FA service configuration by following the steps in the *FA Service Configuration Verification* section.
- Step 8** Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

## FA Service Creation

Use the following example to create the FA service:

**Important:** A maximum of 256 services (regardless of type) can be configured per system.

```
configure

context <fa_ctxt_name> -noconfirm

fa-service <fa_svc_name> -noconfirm]
```

```
end
```

Notes:

- `<fa_ctxt_name>` is name of the context to use for FA service configuraiton. Generally FA should be configured within a destination context.
- `<fa_svc_name>` is name of the FA service where other parameters have to configure for FA functionality.

## IP Interface and UDP Port Binding for Pi Interface

Use the following example to bind the FA service to an local IP interface and specify the maximum number of subscribers that can access this service. Binding an interface to the FA service causes the interface to take on the characteristics of a Pi interface.

```
configure
```

```
context <fa_ctxt_name>

fa-service <fa_svc_name>

bind address <fa_ip_address> max-subscribers <max_subs>

ip local-port <udp_port_num>

end
```

Notes:

- `<fa_svc_name>` is name of the FA service which is created to configure FA functionality.
- `<fa_ip_address>` is the local IP address in IPv4/IPv6 notation for providing Pi interface characteristics.
- `<max_subs>` is the maximum number of subscribers that can access this service on this interface. This can be configured to any integer value from 0 to 500,000. The default is 500,000.



**Important:** The maximum number of subscribers supported is dependant on the session capacity license installed and the number of active PACs/PSCs installed in the system. For more information on session capacity license, refer to the Software Management Operations chapter of the System Administration Guide.

- `<udp_port_num>` is the UDP port number from 1 through 65535 to be used for Pi interface. Default port number is 434.
- For more information on commands/keywords that configure additional parameters and options, refer *FA Service Configuration Mode Commands* chapter of *Command Line Interface Reference*.

## Security Parameter Index (SPI) Configuration

Use the following example to configure the security parameter index (SPI) between FA service and HA:



**Important:** A maximum of 2048 FA-HA SPIs can be configured for a single FA service.

```
configure

context <fa_ctxt_name>

    fa-service <fa_svc_name>

        fa-ha-spi remote-address <ha_ip_address> spi-number <spi_num> {encrypted secret
<enc_secret_key> | secret <secret_key>} [description <desc_string>]

    end
```

#### Notes:

- <fa\_svc\_name> is name of the FA service which is created to configure FA functionality.
- <ha\_ip\_address> is the IP address in IPv4/IPv6 notation of HA to which this FA service will interact.
- <spi\_num> specifies the SPI number which indicates a security context between the FA and the HA in accordance with RFC 2002 and can be configured to any integer value from 256 through 4294967295.
- <enc\_secret\_key> specifies the encrypted shared key between the FA and the HA services. It must be from 1 to 127 alpha and/or numeric characters and is case sensitive.



**Important:** The encrypted keyword is intended only for use by the system while saving configuration scripts. The system displays the encrypted keyword in the configuration file as a flag that the variable following the **secret** keyword is the encrypted version of the plain text secret. Only the encrypted secret is saved as part of the configuration file.

- <secret\_key> specifies the secret shared key between the FA and the HA services. It must be from 1 to 127 alpha and/or numeric characters and is case sensitive.
- <desc\_string> is the description for this SPI and must be from 1 to 31 alpha and/or numeric characters.
- For more information on commands/keywords that configure additional parameters and options, refer FA Service Configuration Mode Commands chapter of Command Line Interface Reference.

## FA Agent Advertisement Parameter Configuration

Use the following example to configure the agent advertisement parameters for this FA service:

```
configure

context <fa_ctxt_name>

    fa-service <fa_svc_name>

        advertise adv-lifetime <adv_dur>

        advertise num-adv-sent <adv_num>

        advertise reg-lifetime <reg_dur>

    end
```

#### Notes:

- `<fa_svc_name>` is name of the FA service which is created to configure FA functionality.
- `<advt_dur>` is the amount of time that an FA agent advertisement remains valid in the absence of further advertisements. It is measured in seconds and can be configured to any integer value from 1 to 65535. The default is 9000.
- `<advt_num>` is the number of unanswered agent advertisements that the FA service allows during call setup before it rejects the session. It can be any integer value from 1 to 65535. The default is 3.
- `<reg_dur>` specify the longest registration lifetime that the FA service allows in any Registration Request message from the mobile node. It is measured in seconds and can be configured to any integer value from 1 to 65534. The default is 600.

## Subscriber Registration, Authentication and Timeout Parameter Configuration

Use the following example to configure the number of subscriber registration, authentication procedure and registration timeout parameters for this FA service:

```
configure

  context <fa_ctxt_name>

    fa-service <fa_svc_name>

      multiple-reg <reg_num>

      reg-timeout <timeout_dur>

      authentication mn-aaa {always | ignore-after-handoff | init-reg | init-reg-
except-handoff | renew-and-dereg-noauth | renew-reg-noauth} [optimize-retries]

    end
```

Notes:

- `<fa_svc_name>` is name of the FA service which is created to configure FA functionality.
- `<reg_num>` is the number of simultaneous Mobile IP sessions that are to be supported for a single subscriber. It can be configured to any integer value from 1 to 3. The default value is 1.



**Important:** The system supports multiple Mobile IP sessions per subscriber only if the subscriber's mobile node has a static IP address. The system only allows a single Mobile IP session for mobile nodes that receive a dynamically assigned home IP address.



**Important:** In addition, because only a single Mobile IP or proxy-Mobile IP session is supported for IP PDP contexts, this parameter must remain at its default configuration.

- `<timeout_dur>` is the maximum amount of time that the FA service waits for a Registration Rely message from the HA. It is measured in seconds and can be configured to any integer value from 1 to 65535. The default value is 45.
- For more information on authentication mn-aaa commands/keywords that configure additional parameters and options, refer FA Service Configuration Mode Commands chapter of Command Line Interface Reference.

## Revocation Message Configuration

Use the following example to configure the FA service for controlling the negotiation and sending of the I-bit in revocation messages:

```
configure

  context <fa_ctxt_name>

    fa-service <fa_svc_name>

      revocation negotiate-i-bit

    end
```

Notes:

- By default the system will not send the I-bit in the revocation message.

## FA Service Configuration Verification

**Step 1** Verify that your FA service is configured properly by entering the following command in Exec Mode:

```
show fa-service all
```

The output from this command should look similar to the sample shown below. In this example an FA service named `fa1` was configured in the `isp1` context.

```
Service name:      fa1

Context:          isp1

Bind:             Done                Max Subscribers:    500000

Local IP Address: 195.20.20.3         Local IP Port       434

Lifetime:         00h10m00s          Registration Timeout: 45 (secs)

Advt Lifetime     02h30m00s          Advt Interval:      5000 (msecs)

Num Advt:         5

Advt Prefix Length Extn: NO

Reverse Tunnel:    Enabled            GRE Encapsulation:   Enabled

SPI(s):

FAHA: Remote Addr: 195.30.30.3/32

Hash Algorithm:    HMAC_MD5           SPI Num:    1000

Replay Protection: Timestamp          Timestamp Tolerance: 60
```

IPSEC Crypto Map(s):

Peer HA Addr: 195.30.30.2

Crypto Map: test

Registration Revocation: Enabled Reg-Revocation I bit: Enabled

Reg-Revocation Max Retries: 3 Reg-Revocation Timeout: 3 (secs)

Reg-Rev on InternalFailure: Enabled

**Step 2** Verify configuration for errors in FA service by entering the following command in Exec Mode:

**show configuration errors section fa-service verbose**

# Common Gateway Access Support Configuration

This section describes some advance feature configuration to support multiple access networks (CDMA, eHRPD and LTE) plus a GSM/UMTS for international roaming with the same IP addressing behavior and access to 3GPP AAA for subscriber authorization. Subscribers using static IP addressing will be able to get the same IP address regardless of the access technology.

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

**Important:** This feature is a license-enabled support and you may need to install a feature specific session license on your system to use some commands related to this configuration.

These instructions assume that you have already configured the system level configuration as described in *System Administration Guide* and GGSN service as described in *GGSN Service Configuration* section in this chapter.

To configure the S6b and other advance features:

- Step 1** Configure Diameter endpoint by applying the example configuration in the *Diameter Endpoint Configuration* section.
- Step 2** Create or modify AAA group by applying the example configuration in the *AAA Group Configuration* section.
- Step 3** Modify GGSN service to allow authorization with HSS by applying the example configuration in the *Authorization over S6b Configuration* section.
- Step 4** *Optional.* Create and associate DNS client parameters by applying the example configuration in the *DNS Client Configuration* section.
- Step 5** *Optional.* Modify GGSN service to accept duplicate calls when received with same IP address by applying the example configuration in the *Duplicate Call Accept Configuration* section.
- Step 6** Verify your S6b configuration by following the steps in the *Common Gateway Access Support Configuration Verification* section.
- Step 7** Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

## Diameter Endpoint Configuration

Use the following example to configure the Diameter endpoint:

```
configure

context <ggsn_ctxt_name> -noconfirm

diameter endpoint <s6b_endpoint_name>

origin host <host_name> address <ip_address>

peer <peer_name> realm <realm_name> address <ip_address> port <port_num>
```

```
end
```

Notes:

- `<ggsn_ctxt_name>` is name of the context which contains GGSN service on system.

## AAA Group Configuration

Use the following example create/modify the AAA group for this feature.

```
configure
```

```
context <fa_ctxt_name>

aaa group <aaa_grp_name>

    diameter authentication dictionary aaa-custom15

    diameter authentication endpoint <s6b_endpoint_name>

    diameter authentication server <server_name> priority <priority>

end
```

Notes:

- `<s6b_endpoint_name>` is name of the existing Diameter endpoint.

## Authorization over S6b Configuration

Use the following example to enable the S6b interface on GGSN service with 3GPP AAA/HSS:

```
configure
```

```
context <ggsn_ctxt_name>

ggsn-service <ggsn_svc_name>

    plmn-unlisted-sgsn home

    authorize-with-hss

    fqdn host <host_name> realm <realm_name>

end
```

Notes:

- `<ggsn_svc_name>` is name of the GGSN service which is already created on the system.

## DNS Client Configuration

Use the following example to enable the S6b interface on GGSN service with 3GPP AAA/HSS:



```
configure

context <ggsn_ctxt_name>

    ip domain-lookup

    ip name-servers <ip_address/mask>

    dns-client <dns_name>

    bind address <ip_address>

    resolver retransmission-interval <duration>

    resolver number-of-retries <retrie>

    cache ttl positive <ttd_value>

    exit

ggsn-service <ggsn_svc_name>

    default dns-client context

end
```

**Notes:**

- <ggsn\_svc\_name> is name of the GGSN service which is already created on the system.

## Duplicate Call Accept Configuration

Use the following example to configure GGSN service to accept the duplicate session calls with request for same IP address:

```
configure

context <ggsn_ctxt_name>

    ggsn-service <ggsn_svc_name>

        newcall duplicate-subscriber-requested-address accept

    end
```

**Notes:**

- <ggsn\_svc\_name> is name of the GGSN service which is already created on the system.

## Common Gateway Access Support Configuration Verification

- Step 1** Verify that your common gateway access support is configured properly by entering the following command in Exec Mode:

```
show ggsn-service all
```

The output from this command should look similar to the sample shown below. In this example GGSN service named *GGSN1* was configured in the *vpn1* context.

```
Service name:          ggsn1
Context:              cn1
Associated PGW svc:    None
Associated GTPU svc:   None
Accounting Context Name:cn1
dns-client Context Name:cn1
Authorize:            hss
Fqdn-name:            xyz.abc@starent.networks.com
Bind:                 Not Done
Local IP Address:     0.0.0.0          Local IP Port:      2123
Self PLMN:            Not defined
Retransmission Timeout: 5 (secs)
```

# Rf Interface Configuration for Offline Charging

This section describes the step-by-step procedure for the configurations that are required to setup the Rf interface on GGSN to support offline charging.

These instructions assume that you have already configured the system level configuration as described in *System Administration Guide*, GGSN service as described in *GGSN Service Configuration* section in this chapter.

To configure the Rf interface on GGSN node:

- Step 1** Create and configure the accounting policy by applying the example configuration in the *Accounting Policy Configuration* section.
- Step 2** Configure a AAA group to associate the diameter accounting dictionary with the by applying the example configuration in the *AAA Group Configuration* section.
- Step 3** Configuring an APN to associate the accounting policy by applying the example configuration in *APN Configuration for Rf Interface* section.
- Step 4** Verify your Rf interface configuration by following the steps in the *Rf Interface Configuration Verification*
- Step 5** Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

## Accounting Policy Configuration

Use the following example to configure the accounting policy for this feature:

```
configure
  context <ctxt_name>
    policy accounting <policy_name>
      operator-string <ip_address>
      accounting-level [ sdf | flow ]
      cc profile [ 2 | 4 | 6 | 8 ] [ buckets | interval | sdf-interval | sdf-volume |
serving nodes | tariff | volume ]
    end
```

## Diameter End-Point Configuration

Use the following example to define the diameter accounting end-point and associate a diameter accounting dictionary for this feature:

```
configure
  context <ctxt_name>
```

```
diameter endpoint <endpoint_name>

    origin host <diameter_host_name> address <ip_address>

    peer <peer_name> realm <peer_realm_name>
address <ip_address>
port <port_number>

end
```

## AAA Group Configuration

Use the following example to create/modify the AAA group for this feature:

```
configure

context <ctxt_name>

    aaa group <group_name>

        diameter accounting endpoint <endpoint_name>

        diameter accounting dictionary [ aaa-custom1 | aaa-custom10 | aaa-custom2 | aaa-
custom3 | aaa-custom4 | aaa-custom5 | aaa-custom6 | aaa-custom7 | aaa-custom8 | aaa-
custom9 ]

        diameter accounting server <diameter_hostname> priority <number>

    end
```

## APN Configuration for Rf Interface

Use the following example create/modify the APN configuration for this feature:

```
configure

context <ctxt_name>

    apn <apn_name>

    associate accounting-policy <policy_name>

end
```

## Rf Interface Configuration Verification

Verify that your Rf interface configuration for offline charging support is configured properly by entering the following command in Exec Mode:

```
show configuration context <ctxt_name>
```

The output from this command should look similar to the sample shown below. In this example accounting policy named *test\_policy* was configured in the *rf\_context* context.

```
config

context rf_context

  subscriber default

  exit

  apn apn

    associate accounting-policy test_policy

  exit

  aaa group default

  #exit

  aaa group rf_aaa

    diameter accounting dictionary aaa-custom6

    diameter accounting endpoint rf_endpoint

    diameter accounting server rf_server priority 2

  #exit

  gtpv group default

  #exit

  policy accounting test_policy

    accounting-level flow

    operator-string Rf_string

    cc profile 2 buckets 5

  #exit

  diameter endpoint rf_endpoint

    origin host rf_diameter address 1.2.3.4

    peer ak realm ak_realm address 2.3.4.5 port 52

  #exit

  ip igmp profile default

  #exit
```

**Rf Interface Configuration for Offline Charging**

```
#exit  
end
```

# Chapter 7

## Monitoring the Service

---

This chapter provides information for monitoring service status and performance using the **show** commands through the Command Line Interface (CLI).

These command have many related keywords that allow them to provide useful information on all aspects of the system ranging from current software configuration through call activity and status.

The selection of keywords described in this chapter is intended to provided the most useful and in-depth information for monitoring the system. For additional information on these and other **show** command keywords, refer to the *Command Line Interface Reference*.

In addition to the CLI, the system supports the sending of Simple Network Management Protocol (SNMP) traps that indicate status and alarm conditions. Refer to the *SNMP MIB Reference Guide* for a detailed listing of these traps.

# Monitoring System Status and Performance


This section contains commands used to monitor the status of tasks, managers, applications and other software components in the system.

Output descriptions for most of the commands are located in the *Statistics and Counters Reference*.

**Table 15. System Status and Performance Monitoring Commands**

To do this:	Enter this command:
<b>View Subscriber Information</b>	
Display Session Resource Status	
View session resource status	<code>show resources session</code>
Display Subscriber Configuration Information	
View locally configured subscriber profile settings (must be in context where subscriber resides)	<code>show subscribers configuration username subscriber_name</code>
View remotely configured subscriber profile settings	<code>show subscribers aaa-configuration username subscriber_name</code>
View Subscribers Currently Accessing the System	
View a listing of subscribers currently accessing the system	<code>show subscribers all</code>
View information for all ggsn-only subscriber sessions	<code>show subscribers ggsn-only all</code>
View information for a specific subscriber	<code>show subscribers full username username</code>
View Subscriber Counters	
View counters for a specific subscriber	<code>show subscribers counters username subscriber_name</code>
View Recovered Session Information	
View session state information and session recovery status	<code>show subscriber debug-info { callid   msid   username }</code>
<b>View Session Statistics and Information</b>	
Display Historical Session Counter Information	
View all historical information for all sample intervals	<code>show session counters historical</code>
Display Session Duration Statistics	
View session duration statistics	<code>show session duration</code>
Display Session State Statistics	
View session state statistics	<code>show session progress</code>
Display Session State PCF Statistics	



To do this:	Enter this command:
View session state PCF statistics	<code>show session progress pcf all</code>
Display Session Subsystem and Task Statistics	
 <b>Important:</b> Refer to the <i>System Software Task and Subsystem Descriptions</i> of the <i>System Administration Guide</i> for additional information on the Session subsystem and its various manager tasks.	
View AAA Manager statistics	<code>show session subsystem facility aaamgr all</code>
View FA Manager statistics	<code>show session subsystem facility famgr all</code>
View GTPC Manager statistics	<code>show session subsystem facility gtpcmgr all</code>
View L2TP demux manager statistics	<code>show session subsystem facility l2tpdemux all</code>
View L2TP Manager statistics	<code>show session subsystem facility l2tpmgr all</code>
View Session Manager statistics	<code>show session subsystem facility sessmgr all</code>
Display Session Disconnect Reasons	
View session disconnect reasons with verbose output	<code>show session disconnect-reasons</code>
<b>View Point-to-Point Protocol Statistics</b>	
Display a Summary of PPP Counter Status	
View cumulative subscriber session PPP counters	<code>show ppp</code>
Display PPP Counters for a Specific Subscriber	
View individual subscriber session PPP counters	<code>show ppp username subscriber_name</code>
View individual subscriber session PPP error and data counters	<code>show ppp counters username subscriber_name</code>
View individual subscriber session detailed PPP counters	<code>show ppp full username subscriber_name</code>
<b>View Mobile IP Foreign Agent Statistics</b>	
Display Mobile IP FA Information for a Specific Subscriber	
View Mobile IP FA counters for a specific subscriber	<code>show mipfa full username subscriber_name</code>
Display Mobile IP Statistics for FA Services	
View statistics for a specific FA service	<code>show mipfa statistics fa-service service_name</code>
Display Mobile IP FA Counters	

To do this:	Enter this command:
View Mobile IP FA counters for individual subscriber sessions	<b>show mipfa counters</b>
<b>View APN Statistics</b>	
view statistics for all APNs within a context	<b>show apn statistics</b>
view statistics for an individual APN	<b>show apn statistics name</b> <i>isp2</i>
<b>View DHCP Information and Counters</b>	
Display DHCP Counter Information	
View DHCP counter information for a specific DHCP service	<b>show dhcp dhcp-service</b> <i>svc_name</i>
View DHCP counter information for a specific DHCP user	<b>show dhcp counter user-address</b> <i>address</i>
Display DHCP Server Statistics	
View statistics for all configured DHCP servers within the context	<b>show dhcp statistics</b>
Display DHCP Status	
View status for all configured DHCP services and servers within the context	<b>show dhcp status</b>
<b>View GTPC Statistics</b>	
View verbose GTP statistics	<b>show gtpc statistics verbose</b>
<b>View GTPP Statistics</b>	
View GTPP statistics for all CGFs	<b>show gtp statistics</b>
View GTPP statistics for a specific CGF	<b>show gtp statistics cgf-address</b> <i>ip_address</i>
<b>View L2TP Information</b>	
Display L2TP Session Information	
View cumulative statistics for all sessions processed within the current context. If this command is executed from within the local context, cumulative session information is displayed for all contexts.	<b>show l2tp sessions</b>
View all information pertaining to the L2TP session of a specific subscriber	<b>show l2tp session full username</b> <i>subscriber_name</i>
Display L2TP Statistics	
View statistics for a specific LAC service. If this command is executed from within the local context, cumulative session information is displayed for all contexts.	<b>show l2tp statistics lac-service</b> <i>service_name</i>
Display L2TP Tunnel Information	
View all tunnels currently being facilitated by LAC services within a specific context	<b>show l2tp tunnels all</b>
Display IPsec Security Association Statistics	
View IPsec security association statistics for crypto maps in the current context	<b>show crypto ipsec security-associations statistics</b>

To do this:	Enter this command:
Display Pre-shared ISAKMP Keys	
View pre-shared keys received from peer security gateways as part of the Diffie-Hellman exchange	<b>show crypto isakmp keys</b>
Display IPSec Statistics	
View cumulative IPSec statistics for the current context	<b>show crypto statistics</b>

## Clearing Statistics and Counters

It may be necessary to periodically clear statistics and counters in order to gather new information. The system provides the ability to clear statistics and counters based on their grouping (PPP, MIPHA, MIPFA, etc.).

Statistics and counters can be cleared using the CLI **clear** command. Refer to *Command Line Interface Reference* for detailed information on using this command.

# Chapter 8

## Configuring Subscriber Session Trace Support

---

This chapter provides information on subscriber session trace functionality to allow an operator to trace subscriber activity at various points in the network and at various level of details in UMTS network. The product Administration Guides provide examples and procedures for configuration of basic services on the system. It is recommended that you select the configuration example that best meets your service model, and configure the required elements for that model, as described in the respective product Administration Guide, before using the procedures in this chapter.



**Important:** The features described in this chapter are an enhanced feature and need enhanced feature license. This support is only available if you have purchased and installed particular feature support license on your chassis.

---

This chapter discusses following topics for feature support of Subscriber Session Tracing in GGSN service:

- [Introduction](#)
- [Supported Standards](#)
- [Supported Networks and Platforms](#)
- [Licenses](#)
- [Subscriber Session Trace Functional Description](#)
- [Subscriber Session Trace Configuration](#)
- [Verifying Your Configuration](#)

# Introduction

The Subscriber Level Trace provides a 3GPP standards-based session-level trace function for call debugging and testing new functions and access terminals in an UMTS environment.

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

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

- Management initiation via direct CLI configuration
- Management initiation at AAA with trace activation via authentication response messages over **Gx** reference interface
- Signaling based activation through signaling from subscriber access terminal



**Important:** Once the trace is provisioned it can be provisioned through the access cloud via various signaling interfaces.

---

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

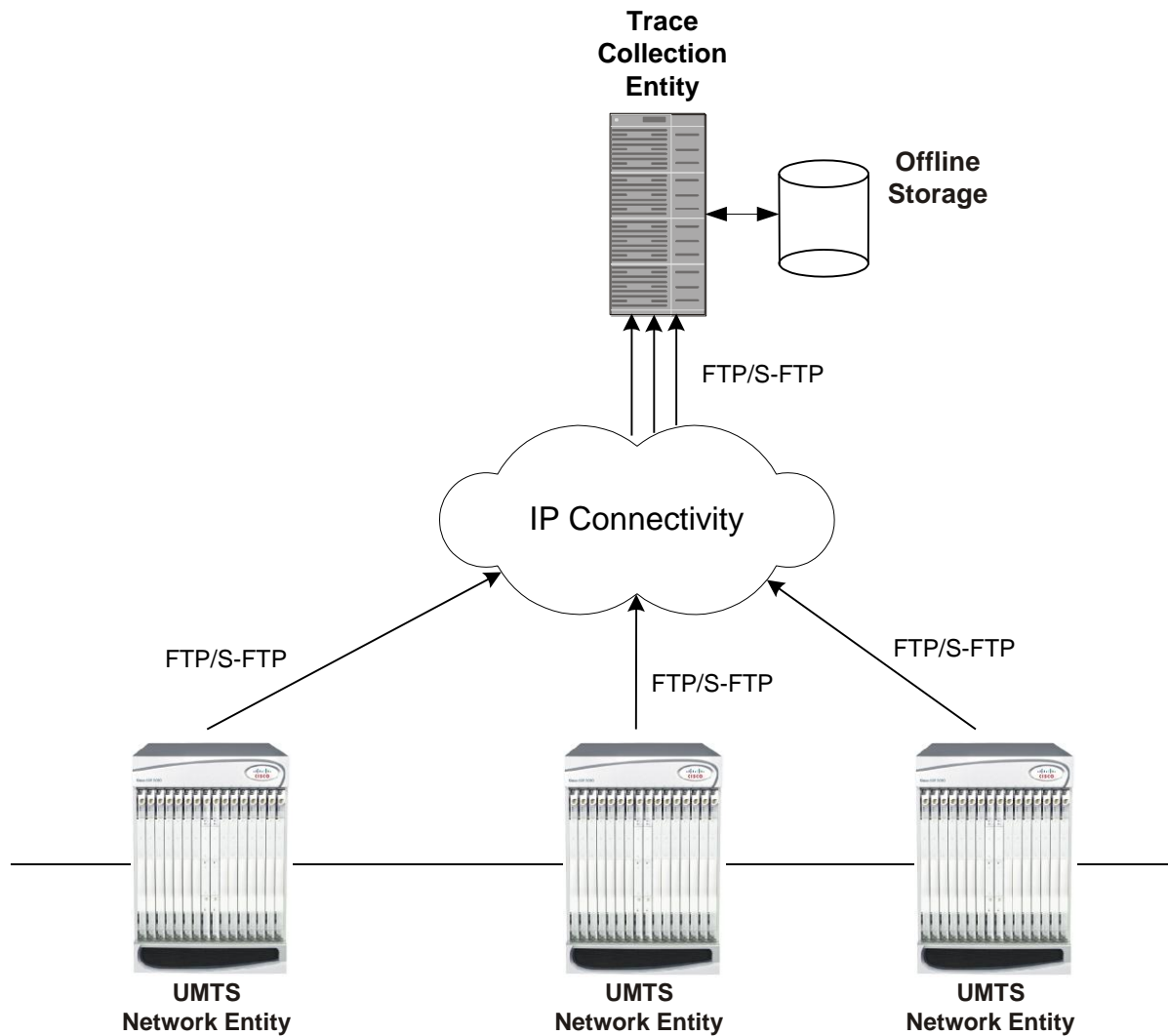


**Important:** Only Maximum Trace Depth is supported in the current release.

---

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

Figure 34. Session Trace Function and Interfaces



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

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

## Supported Functions

This section provides the list of supported functionality of this feature support:

- Support to trace the control flow through the access/core network.
  - Trace of specific subscriber identified by IMSI
  - Trace of UE identified by IMEI(SV)
- Management and Signaling-based activation models

- Ability to specify specific functional entities and interfaces where tracing should occur.
- Scalability and capacity
  - Support up to 32 simultaneous session traces per NE
  - Capacity to activate/deactivate **TBD** trace sessions per second
  - Each NE can buffer **TBD** bytes of trace data locally
- Node and subscriber level statistics and subscriber state Support
- Session Trace Details
- Trace Parameter Propagation
- Trace interfaces in GGSN - Gn, Gi, Gx, and Gmb
- Trace Depth: Maximum, Minimum, Medium (with or without vendor extension)
- XML Encoding of Data as per 3GPP standard 3GPP TS 32.422 V8.6.0 (2009-09)
- Trace Data Collection/Encoding/Forwarding
- Tracing of PDP/MBMS call
- Trace continuity during Gn/Gp handoff
- Trace Collection Entity (TCE) Support
  - Active pushing of files to the TCE
  - Passive pulling of files by the TCE
- 1 TCE support per context
- Trace Session Recovery after Failure of Session Manager



## Supported Standards

Support for the following standards and requests for comments (RFCs) have been added with this interface support:

- 3GPP TS 32.421 V8.5.0 (2009-06): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Subscriber and equipment trace: Trace concepts and requirements (Release 8)
- 3GPP TS 32.422 V8.6.0 (2009-09): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Subscriber and equipment trace; Trace control and configuration management (Release 8)
- 3GPP TS 32.423 V8.2.0 (2009-09): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Subscriber and equipment trace: Trace data definition and management (Release 8)

## Supported Networks and Platforms

This feature supports all systems with StarOS Release 11.0 or later running GGSN service(s) for the core UMTS network functions.

# Licenses

This is a base feature and available for configuration with default GGSN component license(s) on the system:

# Subscriber Session Trace Functional Description

This section describes the various functionality involved in tracing of subscriber session on UMTS nodes:

## Operation

The session trace functionality is separated into two steps - activation and trigger.

Before tracing can begin, it must be activated. Activation is done either via management request or when a UE initiates a signaled connection. After activation, tracing actually begins when it is triggered (defined by a set of trigger events).

## Trace Session

A trace session is the time between trace activation and trace de-activation. It defines the state of a trace session, including all user profile configuration, monitoring points, and start/stop triggers. It is uniquely identified by a Trace Reference.

The Trace Reference id is composed of the MCC (3 digits) + the MNC (3 digits) + the trace Id (3 byte octet string).

## Trace Recording Session

A trace recording session is a time period in which activity is actually being recorded and traceable data is being forwarded to the TCE. A trace recording session is initiated when a start trigger event occurs and continues until the stop trigger event occurs and is uniquely identified by a Trace Recording Session Reference.

## Network Element (NE)

Network elements are the functional component to facilitate subscriber session trace in mobile network.

The term network element refers to a functional component that has standard interfaces in and out of it. It is typically shown as a stand-alone GSN. Examples of NEs are the GGSN and SGSN.

Currently subscriber session trace is not supported for co-located network elements in UMTS network.

## Activation

Activation of a trace is similar whether it be via the management interface or via a signaling interface. In both cases, a trace session state block is allocated which stores all configuration and state information for the trace session. In addition, a (S)FTP connection to the TCE is established if one does not already exist (if this is the first trace session established, odds are there will not be a (S)FTP connection already established to the TCE).

If the session to be traced is already active, tracing may begin immediately. Otherwise, tracing activity concludes until the start trigger occurs (typically when the subscriber/UE under trace initiates a connection). A failure to activate a trace (due to max exceeded or some other failure reason) results in a notification being sent to the TCE indicating the failure.

## Management Activation

With a management-initiated activation, the WEM sends an activation request directly to the NE where the trace is to be initiated. The NE establishes the trace session and waits for a triggering event to start actively tracing. Depending upon the configuration of the trace session, the trace activation may be propagated to other NEs.

## Signaling Activation

With a signaling based activation, the trace session is indicated to the NE across a signaling interface via a trace invocation message. This message can either be piggybacked with an existing bearer setup message (in order to trace all control messages) or by sending a separate trace invocation message (if the user is already active).

## Start Trigger

A trace recording session starts upon reception of one of the configured start triggers. Once the start trigger is received, the NE generates a Trace Recording Session Reference (unique to the NE) and begins to collect and forward trace information on the session to the TCE.

List of trigger events are listed in 3GPP standard 3GPP TS 32.422 V8.6.0 (2009-09).

## Deactivation

Deactivation of a Trace Session is similar whether it was management or signaling activated. In either case, a deactivation request is received by the NE that contains a valid trace reference results in the de-allocation of the trace session state block and a flushing of any pending trace data. In addition, if this is the last trace session to a particular TCE, the (S)FTP connection to the TCE is released after the last trace file is successfully transferred to the TCE.

## Stop Trigger

A trace recording session ends upon the reception of one of the configured stop triggers. Once the stop trigger is received, the NE will terminate the active recording session and attempt to send any pending trace data to the TCE. The list of triggering events can be found in 3GPP standard 3GPP TS 32.422 V8.6.0 (2009-09).

## Data Collection and Reporting

Subscriber session trace functionality supports data collection and reporting system to provide historical usage and event analysis.

All data collected by the NE is formatted into standard XML file format and forwarded to the TCE via (S)FTP. The specific format of the data is defined in 3GPP standard 3GPP TS 32.423 V8.2.0 (2009-09)

## Trace Depth

The Trace Depth defines what data is to be traced. There are six depths defined: Maximum, Minimum, and Medium all having with and without vendor extension flavors. The maximum level of detail results in the entire control message getting traced and forwarded to the TCE. The medium and minimum define varying subsets of the control messages

(specific decoded IEs) to be traced and forwarded. The contents and definition of the medium and minimum trace can be found in 3GPP standard 3GPP TS 32.423 V8.2.0 (2009-09).

Note: Only Maximum Trace Depth is supported in the current release.

## Trace Scope

The Trace Scope defines what NEs and what interfaces have the tracing capabilities enabled on them. This is actually a specific list of NE types and interfaces provided in the trace session configuration by the operator (either directly via a management interface or indirectly via a signaling interface).

## Network Element Details

Trace functionality for each of the specific network elements supported by this functionality are described in this section.

This section includes the trace monitoring points applicable to them as well as the interfaces over which they can send and/or receive trace configuration.

## GGSN

The GGSN support tracing of the following interfaces with the following trace capabilities:

Interface Name	Remote Device	Trace Signaling	Trace Management
Gn (GTP v1 and v0)	SGSN	Y	Y
Gi	RADIUS Server	Y	Y
Gx	PCRF	-	Y
Gmb	BM-SC	N	Y

## Subscriber Session Trace Configuration

This section provides a high-level series of steps and the associated configuration examples for configuring the system to enable the Subscriber Session Trace collection and monitoring function on network elements in UMTS networks.



**Important:** This section provides the minimum instruction set to enable the Subscriber Session Trace functionality to collect session traces on network elements on UMTS networks. Commands that configure additional function for this feature are provided in the *Command Line Interface Reference*.

These instructions assume that you have already configured the system level configuration as described in the *System Administration Guide* and specific product Administration Guide.

To configure the system to support subscriber session trace collection and trace file transport on a system:

- Step 1** Enable the subscriber session trace functionality with NE interface and TCE address at the Exec Mode level on an UMTS network element by applying the example configurations presented in the *Enabling Subscriber Session Trace on UMTS Network Element* section.
- Step 2** Configure the network and trace file transportation parameters by applying the example configurations presented in the *Trace File Collection Configuration* section.
- Step 3** Configure the Trace Collection Entity (TCE) which is required, if session trace is configured for PUSH with **tce-mode** during signalling activation, in GGSN service configuration mode by applying the example configurations presented in the *Trace Collection Entity Configuration* section.
- Step 4** Save the changes to system configuration by applying the example configuration found in *Verifying and Saving Your Configuration* chapter.
- Step 5** Verify the configuration of Subscriber Session Trace related parameters by applying the commands provided in the *Verifying Your Configuration* section of this chapter.

## Enabling Subscriber Session Trace on UMTS Network Element

This section provides the configuration example to enable the subscriber session trace on a system at the Exec mode:

```
session trace subscriber network-element ggsn {imei <imei_id>} {imsi <imsi_id>}
{interface {all | <interface>}} trace-ref <trace_ref_id> collection-entity
<ip_address>
```

Notes:

- *<interface>* is the name of the interfaces applicable for specific NE on which subscriber session traces have to be collected. For more information, refer **session trace subscriber** command in the *Command Line Interface Reference*.
- *<trace\_ref\_id>* is the configured Trace Id to be used for this trace collection instance. It is composed of MCC (3 digit)+MNC (3 digit)+Trace Id (3 byte octet string).
- *<ip\_address>* is the IP address of Trace collection Entity in IPv4 notation.

## Trace File Collection Configuration

This section provides the configuration example to configure the trace file collection parameters and protocols to be used to store trace files on TCE through FTP/S-FTP:

```
configure

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

end
```

Notes:

- *<string>* is the location/path on the trace collection entity (TCE) where trace files will be stored on TCE. For more information, refer **session trace** command in the *Command Line Interface Reference*.

## Trace Collection Entity Configuration

This section provides the configuration example to configure the Trace Collection Entity parameters in GGSN service:

```
configure

  context <ggsn_ctx_name>

    ggsn-service <ggsn_svc_name>

      trace-collection-entity <ipv4-addr> <tce_ip_address>

    end
```

Notes:

- *<ggsn\_svc\_name>* is the GGSN service name for which trace collection entity (TCE) is to be configured.



## Verifying Your Configuration

This section explains how to display and review the configurations after saving them in a *.cfg* file as described in Saving Your Configuration chapter of this guide and also to retrieve errors and warnings within an active configuration for a service.



**Important:** All commands listed here are under Exec mode. Not all commands are available on all platforms.

These instructions are used to verify the Subscriber Session Trace configuration.

**Step 1** Verify that your subscriber session support is configured properly by entering the following command in Exec Mode:

```
show session trace statistics
```

The output of this command displays the statistics of the session trace instance.

```
Num current trace sessions: 5
Total trace sessions activated: 15
Total Number of trace session activation failures: 2
Total Number of trace recording sessions triggered: 15
Total Number of messages traced: 123
Number of current TCE connections: 2
Total number of TCE connections: 3
Total number of files uploaded to all TCEs: 34
```

**Step 2** View the session trace references active for various network elements in an UMTS network by entering the following command in Exec Mode:

```
show session trace trace-summary
```

The output of this command displays the summary of trace references for all network elements:

```
GGSN
Trace Reference: 310012012345
Trace Reference: 310012012346
```



# Chapter 9

## Troubleshooting the Service

---

This chapter provides information and instructions for using the system command line interface (CLI) for troubleshooting issues that may arise during service operation.

# Test Commands

In the event that an issue was discovered with an installed application or line card, depending on the severity, it may be necessary to take corrective action.

The system provides several redundancy and fail-over mechanisms to address issues with application and line cards in order to minimize system downtime and data loss. These mechanisms are described in the sections that follow.

## Using the PPP Echo-Test Command

The system provides a mechanism to verify the Point-to-Point Protocol session of a particular subscriber by sending Link Control Protocol (LCP) packets to the mobile node. This functionality can be extremely useful in determining the quality of the air link and delays that may occur.

The command has the following syntax:

```
ppp echo-test { callid call_id | ipaddr ip_address | msid ms_id | username
subscriber_name }
```

Keyword/Variable	Description
<b>callid</b> <i>call_id</i>	Specifies that the test is executed for a subscriber with a specific call identification number (callid). <i>call_id</i> is the specific call identification number that you wish to test.
<b>ipaddr</b> <i>ip_address</i>	Specifies that the test is executed for a subscriber with a specific IP address. <i>ip_address</i> is the specific IP address that you wish to test.
<b>msid</b> <i>ms_id</i>	Specifies that the test is executed for a subscriber with a specific mobile station identification (MSID) number. <i>ms_id</i> is the specific mobile station identification number that you wish to test.
<b>username</b> <i>subscriber_name</i>	Specifies that the test is executed for a subscriber with a specific username. <i>subscriber_name</i> is the specific username that you wish to test.

The following figure displays a sample of this command's output showing a successful PPP echo-test to a subscriber named user2@aaa.

```
USERNAME: user2@aaa MSID: 0000012345 CALLID: 001e8481

Tx/Rx 1/0 RTT(min/max/avg) 0/0/0


USERNAME: user2@aaa MSID: 0000012345 CALLID: 001e8481

Tx/Rx 1/1 RTT(min/max/avg) 77/77/77 (COMPLETE)
```

## Using the GTPC Test Echo Command

This command tests the GGSN's ability to exchange GPRS Tunneling Protocol control plane (GTP-C) packets with the specified SGSNs which can be useful troubleshooting and/or monitoring.

The test is performed by the system sending GTP-C echo request messages to the specified SGSN(s) and waiting for a response.

 **Important:** This command must be executed from within the context in which at least one GGSN service is configured.

The command has the following syntax:

```
gtpc test echo src-address gn_address { all | sgsn-address ip_address }
```

Keyword/Variable	Description
<b>echo src-address</b> <i>gn_address</i>	Specifies the IP address of a Gn interface configured on the system. <b>NOTE:</b> The IP address of the system's Gn interface must be bound to a configured GGSN service prior to executing this command.
<b>all</b>	Specifies that GTP-C echo requests will be sent to all SGSNs that currently have sessions with the GGSN service.
<b>sgsn-address</b> <i>ip_address</i>	Specifies that GTP-C echo requests will be sent to a specific SGSN. <i>ip_address</i> is the address of the SGSN receiving the requests.


The following example displays a sample of this command's output showing a successful GTPC echo-test from a GGSN service bound to address 192.168.157.32 to an SGSN with an address of 192.168.157.2.

```
GTPC test echo
-----
SGSN: 192.168.157.2 Tx/Rx: 1/1 RTT(ms): 1 (COMPLETE) Recovery:202 (0xCA)
```

## Using the GTPU Test Echo Command

This command tests the GGSN's ability to exchange GPRS Tunneling Protocol user plane (GTP-U) packets with the specified SGSNs which can be useful troubleshooting and/or monitoring.

The test is performed by the system sending GTP-U echo request messages to the specified SGSN(s) and waiting for a response.

 **Important:** This command must be executed from within the context in which at least one GGSN service is configured.

The command has the following syntax:

```
gtpu test echo src-address gn_address { all | sgsn-address ip_address }
```

Keyword/Variable	Description
<b>src-address</b> <i>gn_address</i>	Specifies the IP address of a Gn interface configured on the system. <b>NOTE:</b> The IP address of the system's Gn interface must be bound to a configured GGSN service prior to executing this command.
<b>all</b>	Specifies that GTP-U echo requests will be sent to all SGSNs that currently have sessions with the GGSN service.

Keyword/Variable	Description
<b>sgsn-address</b> <i>ip_address</i>	Specifies that GTP-U echo requests will be sent to a specific SGSN. <i>ip_address</i> is the address of the SGSN receiving the requests.

The following figure displays a sample of this command's output showing a successful GTPU echo-test from a GGSN service bound to address 192.168.157.32 to an SGSN with an address of 192.168.157.2.

```
GTPU test echo
-----
SGSN: 192.168.157.2 Tx/Rx: 1/1 RTT(ms): 24 (COMPLETE)
```

## Using the GTPv0 Test Echo Command

This command tests the GGSN's ability to exchange GPRS Tunneling Protocol version 0 (GTPv0) packets with the specified SGSNs which can be useful troubleshooting and/or monitoring.

The test is performed by the system sending GTPv0 echo request messages to the specified SGSN(s) and waiting for a response.



**Important:** This command must be executed from within the context in which at least one GGSN service is configured.

The command has the following syntax:

```
gtpv0 test echo src-address gn_address { all | sgsn-address ip_address }
```

Keyword/Variable	Description
<b>src-address</b> <i>gn_address</i>	Specifies the IP address of a Gn interface configured on the system. <b>NOTE:</b> The IP address of the system's Gn interface must be bound to a configured GGSN service prior to executing this command.
<b>all</b>	Specifies that GTPv0 echo requests will be sent to all SGSNs that currently have sessions with the GGSN service.
<b>sgsn-address</b> <i>ip_address</i>	Specifies that GTPv0 echo requests will be sent to a specific SGSN. <i>ip_address</i> is the address of the SGSN to receiving the requests.


The following figure displays a sample of this command's output showing a successful GTPv0 echo-test from a GGSN service bound to address 192.168.157.32 to an SGSN with an address of 192.168.157.2.

```
GTPv0 test echo
-----
SGSN: 192.168.157.2 Tx/Rx: 1/1 RTT(ms):14 (COMPLETE) Recovery: 210(0xD2)
```

# Using the DHCP Test Command

This command tests the system's ability to communicate with a Dynamic Host Control Protocol (DHCP) server. Testing is performed on a per-DHCP service basis for either a specific server or all servers the DHCP service is configured to communicate with. This functionality is useful for troubleshooting and/or monitoring.

Once executed, the test attempts to obtain an IP address from the DHCP server(s) and immediately release it.

 **Important:** This command must be executed from within the context in which at least one GGSN service is configured.

The command has the following syntax:

```
dhcp test dhcp-service svc_name [ all | server ip_address ]
```

Keyword/Variable	Description
<b>dhcp-service</b> <i>svc_name</i>	The name of the DHCP service. <i>svc_name</i> can be from 1 to 63 alpha and/or numeric characters in length and is case sensitive.
<b>all</b>	Tests DHCP functionality for all servers.
<b>server</b> <i>ip_address</i>	Tests DHCP functionality for the server.

The following figure displays a sample of this command's output showing a successful DHCP test for a DHCP service called DHCP-Gi to a server with an IP address of 192.168.16.2. The IP address provided during the test was 192.168.16.144.


```
DHCP test status for service <DHCP-Gi>:

Server address: 192.168.16.2 Status: Tested

Lease address: 192.168.16.144 Lease Duration: 600 secs.
```

# Testing GTPP Accounting with a CGF

When used to test a CGF, this tool causes the system to send GTPP echo packets to the specified CGF(s).

 **Important:** This tool must be executed from the context in which GTPP functionality is configured.

To execute the GTPP accounting test tool enter the following command:


```
gtp test accounting { all | cgf-server ip_address }
```

Keyword/Variable	Description
<b>all</b>	Tests all CGFs configured within the given context.
<b>cgf-server</b> <i>ip_address</i>	Tests a specific CGF configured within the given context.

The command's response will display whether the CGF is active or unreachable.

# Testing GTPP Connectivity with a GSS

When used to test a GTPP Storage Server, this tool causes the system to send GTPP echo packets to the specified GSS for checking connectivity and provide round trip time.

 **Important:** This tool must be executed from the context in which GTPP functionality is configured.

To execute the GSS connectivity test tool enter the following command:

```
gtpptest storage-server [address ip-address port udp-port]
```

Keyword/Variable	Description
storage-server	Tests configured GSS within the given context.
address ip_address port udp_port	Tests connectivity with GSS having ip_address and udp_port before configuring it within the given context.

The command’s response will display whether the GSS is active or unreachable.



# Chapter 10

## Mobile-IP and Proxy-MIP Timer Considerations

---

This appendix is intended to provide a brief explanation of the considerations for lifetime, idle, and absolute timer settings that must be understood when setting up a system in a mobile IP or proxy mobile IP environment. In the Cisco ASR5x00 platform, there is not an explicitly defined MIP lifetime. The MIP lifetime is determined through various timers settings in the configuration and through radius attributes returned in an Access-Accept message.

## Call Flow Summary

The following steps describe the call flow as regards the timers that affect a call initiated by the Mobile Node (MN).

1. **PPP Negotiation:** A data call is initiated by beginning PPP. Once PPP is successfully established, the system will understand if the call is a mobile IP call or simple IP call. At this point, the system is not aware of the subscriber username and will use settings from the default subscriber template in the source context or the context defined by the “aaa default-domain subscriber” setting in the global configuration.
2. **FA Agent Advertisement:** Once the system has determined the call is a Mobile IP call, the FA will send a Router Advertisement message with a Mobility Agent Advertisement extension. The Mobility Agent Advertisement includes a Registration Lifetime field. The value of this field will come from one of two places. The FA service has a configurable setting named “advertise reg-lifetime”. The default value for this setting is 600. A setting in the default subscriber template called “timeout idle” is also a candidate. The default value for this setting is 0 (null). The smaller of these two configurable parameters is used as the Registration Lifetime value. Leaving the settings at the defaults will result in an advertised lifetime of 600.

Advertise Reg-Lifetime in FA Service	Timeout Idle in Subscriber Template	Resulting Advertised Registration Lifetime
600	0	600
600	900	600
3600	1200	1200

The device will receive the agent advertisement and send a MIP Registration Request. The device uses the advertised registration lifetime value as the requested MIP lifetime.

3. **AAA Authentication and MIP Registration Request:** The next step in the MIP process will be to authenticate the user at the FA. It is at this stage where a failure condition can be introduced.

If the Access-Accept message does not return any values related to timers, the subscribers MIP Registration Request is sent on to the HA.

If the Access-Accept message does include an attribute relating to Idle or Absolute timer the FA will evaluate the requested lifetime from the device to the value returned by the AAA. The FA will treat any Idle or Absolute timer value returned by the AAA as a maximum value and as such:

- If the requested MIP lifetime from the device is less-than than the returned radius attribute, the lifetime value is considered valid and the MIP Registration Request is forwarded on to the HA.
- If the requested MIP lifetime from the device is greater-than the returned radius attribute, the requested lifetime value is considered to be too long. The FA will send a MIP Registration Reply to the device with a response code of `Error 69 - Requested Lifetime Too Long`. In the reply message, the FA will populate the Lifetime value with the maximum acceptable lifetime. The device may send a new MIP request with this new lifetime value.

MIP Lifetime Requested by Device	Idle-Timer Value in Access-Accept	Resulting MIP Lifetime Request in MIP Request to HA
3600	(Not Returned)	3600
3600	7200	3600
3600	1800	Failure - Error 69

4. **HA Process MIP Request:** The HA has now received a Mobile IP Registration request forwarded by the FA on behalf of the device. The MIP request contains the username and the requested lifetime (as well as other

parameters). The HA will take this lifetime request and compare it to the configurable parameters associated with the HA service and associated configurations. The HA will use the username to determine which subscriber template to use for subscriber specific settings.

The parameters the HA uses to determine the MIP lifetime are the requested lifetime, the “reg-lifetime” setting in the HA service and the “timeout idle” setting in the subscriber template. If the requested MIP lifetime is lower it is sent back to the mobile; if the MIP lifetime is higher the system sends back an RRQ accept with the lifetime set to 5 seconds less than the lower of the idle or absolute timeout for the user.

MIP Lifetime Requested by Device	Timeout Idle/Absolute in Subscriber Template	Reg-Lifetime Value in HA Service	MIP Lifetime Returned to Mobile Device
3600	0(default)	7200	3600
3600	7200	1805	1800
3600	1705	3600	1700

Timer tables combined

PDSN/FA			HA		
Advertise Reg-Lifetime in FA Service	Timeout Idle/Absolute in Subsc. Template (Source Context)	Idle-Timer Value in Access-Accept	Timeout Idle/Absolute in Subscriber Template(HA Context)	Reg-Lifetime Value in HA Service	Resulting Lifetime Value sent to Mobile Device
600	0(default)	(not returned)	0(default)	7200	600
1800	900	7200	7200	1805	900
3600	1200	3600	1705	3600	1200
1500	3600	1500	0(default)	3600	1500
3600	0(default)	(not returned)	0(default)	2405	2400
3600	0(default)	(not returned)	2005	3600	2000
65534	0(default)	7200	0(default)	3600	Lifetime Too Long


## Dealing with the "Requested Lifetime Too Long" Error Code

In some configurations, a roaming partner may return an "Idler-Timer" attribute in an access-accept whose value is smaller than what a carrier may have configured for its own subscribers. This will result in a "Requested Lifetime Too Long" error message being returned to the device. There are several ways to correct this. One is to use a setting in the FA service configuration. Using the "no limit-reg-lifetime" in the FA service configuration will tell the FA service to allow the MIP lifetime to be greater than the Idle or Absolute timers. The FA will not send Error 69 and continue to process the call. The lifetime value in the MIP Request sent to the HA will still be what was determined in Phase 2.

## Controlling the Mobile IP Lifetime on a Per-Domain Basis

The system does not support the configuration of the MIP lifetime timer on per-domain (context) basis. However, a domain-wide lifetime timer can be achieved by configuring the idle-timeout attribute for the default subscriber for each domain.

---


 **Important:** Mobile IP lifetime settings can be controlled on a per-domain basis **only** in deployments for which the idle timeout attribute for individual subscriber profiles is **not** used during operation.

---

In this configuration, the value of the registration lifetime sent by the system in Agent Advertisements is selected by comparing the configured FA Agent Advertisement lifetime setting, and the idle and/or absolute timeout settings configured for the domain's default subscriber. If the value of the idle and/or absolute timeout parameter is less than the Agent Advertisement lifetime, then the system provides a registration lifetime equal to 5 seconds less than the lowest timer value.

If the idle timeout attribute is configured in individual subscriber profiles, per-domain lifetime control is not possible. In this case, the registration lifetime configured for the FA must be the lower of the two values.

---

 **Important:** Commands used in the examples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the Command Line Interface Reference for complete information regarding all commands.

---

The following is an example CLI command sequence used to configure the Mobile IP lifetime on a per-domain basis.

```
configure
  context <aaa_context_name>
    subscriber default
      ip context-name <abc>
    exit
  subscriber name <ptt.bigco.com>
    timeout idle <3605>
    ip context-name <abc>
  exit
  subscriber name <bigco.com>
    timeout idle <7205>
    ip context-name <abc>
  exit
```

```

domain <ptt.bigco.com> default subscriber <ptt.bigco.com>

domain <bigco.com> default subscriber <bigco.com>

end

configure

context <ha_context_name>

subscriber default

exit    ha-service <ha>

idle-timeout-mode normal      reg-lifetime <7200>

end

configure

context <fa_context_name>

fa-service <fa>

advertise reg-lifetime <7200>

end

```

In the example above, two domains (ptt.bigco.com and bigco.com) are configured. The default subscribers are defined for the two domains respectively. The desired operation requires a Mobile IP lifetime of 1 hour (3600 secs) for the ptt.bigco.com domain, and a lifetime of 2 hours (7200 secs) for the bigco.com domain.

Whenever a subscriber session belonging to the ptt.bigco.com domain arrives, the system uses a Mobile IP lifetime timer value equal to 5 seconds less than the idle timeout configured for the default subscriber because the configured value is less than the registration lifetime value configured for the Agent Advertisement. 5 seconds less than the configured value of 3605 seconds equals 3600 seconds which meets the desired operation.

Whenever a subscriber session belonging to the bigco.com domain arrives, the system uses the configured registration lifetime value as the Mobile IP lifetime in Agent Advertisements because it is less than the configured idle timeout in the default subscriber's profile.

As a general rule, the registration lifetime value on the agent **must** be configured as the highest Mobile IP lifetime that is desired for a subscriber. (In the above example, it would be the subscriber bigco.com.)

Another important factor to consider is that the idle timeout value should be reset on receipt of a renewal request. To support this operation, the system provides the **idle-timeout-mode** configurable in the HA service. The following modes are supported:

- **normal**: Resets the idle timeout value on receipt of Mobile IP user data and control signaling
- **aggressive**: Resets the idle timeout value on receipt of Mobile IP user data only (this is the default behavior)
- **handoff**: Resets the idle timeout value on receipt of Mobile IP user data and upon inter-AGW handoff or inter access technologies

The following optional modifier is also supported:

- **upstream-only**: Only upstream user data (data from the mobile node) resets the idle timer for the session. This is disabled by default.







# Chapter 11

## Engineering Rules

---

This section provides engineering rules or guidelines that must be considered prior to configuring the system for your network deployment.

This appendix describes following engineering rules for GGSN service:

- [APN Engineering Rules](#)
- [DHCP Service Engineering Rules](#)
- [GGSN Engineering Rules](#)
- [GRE Tunnel Interface and VRF Engineering Rules](#)
- [GTP Engineering Rules](#)
- [Interface and Port Engineering Rules](#)
- [Lawful Intercept Engineering Rules](#)
- [MBMS Bearer Service Engineering Rules](#)
- [Service Engineering Rules](#)
- [Subscriber Engineering Rules](#)

## APN Engineering Rules

The following engineering rules apply to APNs:

- APNs must be configured within the context used for authentication.
- A maximum of 1,024 APNs per system can be configured.

## DHCP Service Engineering Rules

The following engineering rule applies to the DHCP Service:

- Up to 8 DHCP servers may be configured per DHCP service.
- A maximum of 3 DHCP server can be tried for a call.

## GGSN Engineering Rules

The following engineering rules apply when the system is configured as a GGSN:

- Gn/Gp interfaces can be configured. That is, if a system context is configured with a GGSN service, then all interfaces in that context may be used.
- Gi interfaces can be configured. That is, if a system context is configured as a destination context for an APN, then all interfaces in that context may be used.
- Ga interfaces. That is, if a system context is configured for GTPP accounting, then all interfaces in that context may be used.
- One GSN-MAP node may be configured per system context (in lieu of Gc).
- Up to 1000 network requested PDP contexts may be configured.
- Up to 8 GTPP groups (excluding the default GTPP group) can be configured per chassis.
- Up to 4 GTPP Storage Servers can be configured per GTPP group.
- Up to 32 GTPP Storage Servers can be configured per system context.
- Up to 511 GRE tunnel interface can be configured per context.

## GRE Tunnel Interface and VRF Engineering Rules

The following engineering rules apply to GRE tunnel interface and VRF contexts:

- A maximum of 511 GRE tunnels are allowed to configure in a context but subject to maximum of 2048 GRE tunnels per chassis.
- A maximum of 250 virtual routing and forwarding (VRF) tables are allowed to configure in a context subject to a maximum of 1024 VRFs per chassis.
- A maximum of 10000 IP routes in Release 9.0 and 16384 IP routes in Release 10.0 onward are supported in a VRF context configuration mode.

## GTP Engineering Rules

The following engineering rules apply to GTP on GGSN:

- A maximum of 11 primary (no secondary) PDP context per subscriber can be configured.
- A maximum of 1 primary and 10 secondary PDP context per subscriber can be configured.

# Interface and Port Engineering Rules

The rules discussed in this section pertain to both the Ethernet 10/100 and Ethernet 1000 Line Cards and the four-port Quad Gig-E Line Card (QGLC) and the type of interfaces they facilitate.

## Pi Interface Rules

This section describes the engineering rules for the Pi interface.

### FA to HA Rules

When supporting Mobile IP, the system can be configured to perform the role of an FA, an HA, or both. This section describes the engineering rules for the Pi interface when using the system as a FA.

The following engineering rules apply to the Pi interface between the FA and HA:

- A Pi interface is created once the IP address of a logical interface is bound to an FA service.
- The logical interface(s) that will be used to facilitate the Pi interface(s) must be configured within the egress context.
- FA services must be configured within the egress context.
- If the system is configured as a FA is communicating with a system configured as an HA, then it is recommended that the name of the context in which the FA service is configured is identical to the name of the context that the HA service is configured in on the other system.
- Each FA service may be configured with the Security Parameter Index (SPI) of the HA that it will be communicating with over the Pi interface.
- Multiple SPIs can be configured within the FA service to allow communications with multiple HAs over the Pi interface. It is best to define SPIs using a netmask to specify a range of addresses rather than entering separate SPIs. This assumes that the network is physically designed to allow this communication.
- Depending on the services offered to the subscriber, the number of sessions facilitated by the Pi interface can be limited.

### HA to FA

The following engineering rules apply to the Pi interface between the HA and FA:

- When supporting Mobile IP, the system can be configured to perform the role of a FA, an HA or both. This section describes the engineering rules for the Pi interface when using the system as an HA.
- A Pi interface is created once the IP address of a logical interface is bound to an HA service.
- The logical interface(s) that will be used to facilitate the Pi interface(s) must be configured within an ingress context.
- HA services must be configured within an ingress context.
- If the system configured as an HA is communicating with a system configured as a FA, then it is recommended that the name of the context in which the HA service is configured is identical to the name of the context that the FA service is configured in on the other system.

- Each HA service may be configured with the Security Parameter Index (SPI) of the FA that it will be communicating with over the Pi interface.
- Multiple SPIs can be configured within the HA service to allow communications with multiple FAs over the Pi interface. It is best to define SPIs using a netmask to specify a range of addresses rather than entering separate SPIs. This assumes that the network is physically designed to allow this communication.
- Each HA service must be configured with a Security Parameter Index (SPI) that it will share with mobile nodes.
- Depending on the services offered to the subscriber, the number of sessions facilitated by the Pi interface can be limited in order to allow higher bandwidth per subscriber.

## GRE Tunnel Interface Rule

The following engineering rules apply to the GRE tunnel interface between two GRE tunnel nodes:

- A maximum of 512 IP tunnels (511 GRE tunnels + 1 not tunnel interfaces) are allowed to configure in a context but subject to a maximum of 2048 GRE tunnels per chassis.



## Lawful Intercept Engineering Rules

The following engineering rules apply to Lawful Intercept on supported AGW service:

- A maximum of 1000 Lawful Intercepts can be performed simultaneously.

## MBMS Bearer Service Engineering Rules

The following engineering rules apply to MBMS bearer services:

- A maximum 225 downlink SGSNs per MBMS bearer service are supported on the system.
- A maximum of 2 BMSC (1 primary and 1 secondary) supported per MBMS bearer service.

# Service Engineering Rules

The following engineering rules apply to services configured within the system:

- A maximum of 256 services (regardless of type) can be configured per system.



**Caution:** Large numbers of services greatly increase the complexity of management and may impact overall system performance (i.e. resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

---

- Up to 2,048 MN-HA and 2048 FA-HA SPIs can be supported for a single HA service.
- Up to 2,048 FA-HA SPIs can be supported for a single FA service.
- The system supports unlimited peer FA addresses per HA.
- The system maintains statistics for a maximum of 8192 peer FAs per HA service.
- If more than 8192 FAs are attached, older statistics are identified and overwritten.
- The system maintains statistics for a maximum of 4096 peer HAs per FA service.
- The total number of entries per table and per chassis is limited to 256.
- Up to 10,000 LAC addresses can be configured per LNS service.



**Caution:** Even though service names can be identical to those configured in different contexts on the same system, this is not a good practice. Having services with the same name can lead to confusion, difficulty in troubleshooting the problems, and make it difficult to understand outputs of **show** commands.

---

## Subscriber Engineering Rules

The following engineering rule applies to subscribers configured within the service:

- Default subscriber templates may be configured on a per FA service basis.

# Appendix A

## CoA, RADIUS DM, and Session Redirection (Hotlining)

---

This chapter describes Change of Authorization (CoA), Disconnect Message (DM), and Session Redirect (Hotlining) support in the system. RADIUS attributes, Access Control Lists (ACLs) and filters that are used to implement these features are discussed. The product administration guides provide examples and procedures for configuration of basic services on the system. It is recommended that you select the configuration example that best meets your service model, and configure the required elements for that model, as described in this Administration Guide, before using the procedures in this chapter.



**Important:** Not all commands and keywords/variables are available or supported. This depends on the platform type and the installed license(s).

---

# RADIUS Change of Authorization and Disconnect Message

This section describes how the system implements CoA and DM RADIUS messages and how to configure the system to use and respond to CoA and DM messages.

## CoA Overview

The system supports CoA messages from the AAA server to change data filters associated with a subscriber session. The CoA request message from the AAA server must contain attributes to identify NAS and the subscriber session and a data filter ID for the data filter to apply to the subscriber session. The filter-id attribute (attribute ID 11) contains the name of an Access Control List (ACL). For detailed information on configuring ACLs, refer to the *IP Access Control Lists* chapter in the *System Administration Guide*.

If the system successfully executes a CoA request, a CoA-ACK message is sent back to the RADIUS server and the data filter is applied to the subscriber session. Otherwise, a CoA-NAK message is sent with an error-cause attribute without making any changes to the subscriber session.



**Important:** Changing ACL and rulebase together in a single CoA is not supported. For this, two separate CoA requests can be sent through AAA server requesting for one attribute change per request.

## DM Overview

The DM message is used to disconnect subscriber sessions in the system from a RADIUS server. The DM request message should contain necessary attributes to identify the subscriber session. If the system successfully disconnects the subscriber session, a DM-ACK message is sent back to the RADIUS server, otherwise, a DM-NAK message is sent with proper error reasons.

## License Requirements

## Enabling CoA and DM

To enable RADIUS Change of Authorization and Disconnect Message:

- Step 1** Enable the system to listen for and respond to CoA and DM messages from the RADIUS server as described in the [Enabling CoA and DM](#) section.
- Step 2** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command `save configuration`. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.
- Step 3** View CoA and DM message statistics as described in the [Viewing CoA and DM Statistics](#) section.



**Important:** Commands used in the configuration examples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases,

other optional commands and/or keyword options are available. Refer to the *Command Line Interface Reference* for complete information regarding all commands. Not all commands and keywords/variables are available or supported. This depends on the platform type and the installed license(s).

## Enabling CoA and DM

Use the following example to enable the system to listen for and respond to CoA and DM messages from the RADIUS server:

### configure

```
context <context_name>

    radius change-authorize-nas-ip <ipv4/ipv6_address>

end
```

### Notes:

- *<context\_name>* must be the name of the AAA context where you want to enable CoA and DM. The AAA context must have been configured as described in the *Configuring Context-Level AAA Functionality* section of the *AAA and GTPP Interface Administration and Reference*.
- A number of optional keywords and variables are available for the **radius change-authorize-nas-ip** command. For more information regarding this command please refer to the *Command Line Interface Reference*.

## CoA and DM Attributes

For CoA and DM messages to be accepted and acted upon, the system and subscriber session to be affected must be identified correctly.

To identify the system, use any one of the following attributes:

- NAS-IP-Address: NAS IP address if present in the CoA/DM request should match with the NAS IP address.
- NAS-Identifier: If this attribute is present, its value should match to the nas-identifier generated for the subscriber session

To identify the subscriber session, use any one of the following attributes.

- If 3GPP2 service is configured the following attribute is used for correlation identifier:
  - 3GPP2-Correlation-ID: The values should exactly match the 3GPP2-correlation-id of the subscriber session. This is one of the preferred methods of subscriber session identification.
- If 3GPP service is configured the following attributes are used for different identifiers:
  - 3GPP-IMSI: International Mobile Subscriber Identification (IMSI) number should be validated and matched with the specified IMSI for specific PDP context.
  - 3GPP-NSAPI: Network Service Access Point Identifier (NSAPI) should match to the NSAPI specified for specific PDP context.
- User-Name: The value should exactly match the subscriber name of the session. This is one of the preferred methods of subscriber session identification.
- Framed-IP-Address: The values should exactly match the framed IP address of the session.
- Calling-station-id: The value should match the Mobile Station ID.

To specify the ACL to apply to the subscriber session, use the following attribute:

- **Filter-ID:** CoA only. This must be the name of an existing Access Control List. If this is present in a CoA request, the specified ACL is immediately applied to the specified subscriber session. The Context Configuration mode command, **radius attribute filter-id direction**, controls in which direction filters are applied.

The following attributes are also supported:

- **Event-Timestamp:** This attribute is a timestamp of when the event being logged occurred.
- If 3GPP2 service is configured following additional attributes are supported:
  - **3GPP2-Disconnect-Reason:** This attribute indicates the reason for disconnecting the user. This attribute may be present in the RADIUS Disconnect-request Message from the Home Radius server to the PDSN.
  - **3GPP2-Session-Termination-Capability:** When CoA and DM are enabled by issuing the radius change-authorize-nas-ip command, this attribute is included in a RADIUS Access-request message to the Home RADIUS server and contains the value 3 to indicate that the system supports both Dynamic authorization with RADIUS and Registration Revocation for Mobile IPv4. The attribute is also included in the RADIUS Access-Accept message and contains the preferred resource management mechanism by the home network, which is used for the session and may include values 1 through 3.

## CoA and DM Error-Cause Attribute

The Error-Cause attribute is used to convey the results of requests to the system. This attribute is present when a CoA or DM NAK or ACK message is sent back to the RADIUS server.

The value classes of error causes are as follows:

- 0-199, 300-399 reserved
- 200-299 - successful completion
- 400-499 - errors in RADIUS server
- 500-599 - errors in NAS/Proxy

The following error cause is sent in ACK messages upon successful completion of a CoA or DM request:

- 201- Residual Session Context Removed

The following error causes are sent in NAK messages when a CoA or DM request fails:

- 401 - Unsupported Attribute
- 402 - Missing Attribute
- 403 - NAS Identification Mismatch
- 404 - Invalid Request
- 405 - Unsupported Service
- 406 - Unsupported Extension
- 501 - Administratively Prohibited
- 503 - Session Context Not Found
- 504 - Session Context Not Removable
- 506 - Resources Unavailable



## Viewing CoA and DM Statistics

View CoA and DM message statistics by entering the following command:

**show session subsystem facility aaamgr**

The following is a sample output of this command.

```

1 AAA Managers

807 Total aaa requests                0 Current aaa requests

379 Total aaa auth requests           0 Current aaa auth requests
    0 Total aaa auth probes            0 Current aaa auth probes
    0 Total aaa auth keepalive          0 Current aaa auth keepalive

426 Total aaa acct requests           0 Current aaa acct requests
    0 Total aaa acct keepalive          0 Current aaa acct keepalive

379 Total aaa auth success             0 Total aaa auth failure
    0 Total aaa auth purged             0 Total aaa auth cancelled
    0 Total auth keepalive success       0 Total auth keepalive failure
    0 Total auth keepalive purged
    0 Total aaa auth DMU challenged

367 Total radius auth requests         0 Current radius auth requests
    2 Total radius auth requests retried
    0 Total radius auth responses dropped
    0 Total local auth requests          0 Current local auth requests

12 Total pseudo auth requests          0 Current pseudo auth requests
    0 Total null-username auth requests (rejected)
    0 Total aaa acct completed           0 Total aaa acct purged
    0 Total acct keepalive success       0 Total acct keepalive timeout
    0 Total acct keepalive purged
    0 Total aaa acct cancelled

426 Total radius acct requests         0 Current radius acct requests
    0 Total radius acct requests retried

```

## ■ RADIUS Change of Authorization and Disconnect Message

0 Total radius acct responses dropped	
0 Total gtpa acct requests	0 Current gtpa acct requests
0 Total gtpa acct cancelled	0 Total gtpa acct purged
0 Total null acct requests	0 Current null acct requests
54 Total aaa acct sessions	5 Current aaa acct sessions
3 Total aaa acct archived	0 Current aaa acct archived
0 Current recovery archives	0 Current valid recovery records
2 Total aaa sockets opened	2 Current aaa sockets open
0 Total aaa requests pend socket open	
0 Current aaa requests pend socket open	
0 Total radius requests pend server max-outstanding	
0 Current radius requests pend server max-outstanding	
0 Total aaa radius coa requests	0 Total aaa radius dm requests
0 Total aaa radius coa acks	0 Total aaa radius dm acks
0 Total aaa radius coa naks	0 Total aaa radius dm naks
2 Total radius charg auth	0 Current radius charg auth
0 Total radius charg auth succ	0 Total radius charg auth fail
0 Total radius charg auth purg	0 Total radius charg auth cancel
0 Total radius charg acct	0 Current radius charg acct
0 Total radius charg acct succ	0 Total radius charg acct purg
0 Total radius charg acct cancel	
357 Total gtpa charg	0 Current gtpa charg
357 Total gtpa charg success	0 Total gtpa charg failure
0 Total gtpa charg cancel	0 Total gtpa charg purg
0 Total prepaid online requests	0 Current prepaid online requests
0 Total prepaid online success	0 Current prepaid online failure
0 Total prepaid online retried	0 Total prepaid online cancelled
0 Current prepaid online purged	
0 Total aaamgr purged requests	

```
0 SGSN: Total db records
0 SGSN: Total sub db records
0 SGSN: Total mm records
0 SGSN: Total pdp records
0 SGSN: Total auth records
```

# Session Redirection (Hotlining)

## Overview

Session redirection provides a means to redirect subscriber traffic to an external server by applying ACL rules to the traffic of an existing or a new subscriber session. The destination address and optionally the destination port of TCP/IP or UDP/IP packets from the subscriber are rewritten so the packet is forwarded to the designated redirected address. Return traffic to the subscriber has the source address and port rewritten to the original values. The redirect ACL may be applied dynamically by means of the RADIUS Change of Authorization (CoA) feature.

Note that the session redirection feature is only intended to redirect a very small subset of subscribers at any given time. The data structures allocated for this feature are kept to the minimum to avoid large memory overhead in the session managers.

## License Requirements

## Operation

### ACL Rule

An ACL rule named **readdress server** supports redirection of subscriber sessions. The ACL containing this rule must be configured in the destination context of the user. Only TCP and UDP protocol packets are supported. The ACL rule allows specifying the redirected address and an optional port. The source and destination address and ports (with respect to the traffic originating from the subscriber) may be wildcarded. If the redirected port is not specified, the traffic will be redirected to the same port as the original destination port in the datagrams. For detailed information on configuring ACLs, refer to the *IP Access Control Lists* chapter in the *System Administration Guide*. For more information on **readdress server**, refer to the *ACL Configuration Mode Commands* chapter of the *Command Line Interface Reference*.

## Redirecting Subscriber Sessions

An ACL with the **readdress server** rule is applied to an existing subscriber session through CoA messages from the RADIUS server. The CoA message contains the 3GPP2-Correlation-ID, User-Name, Acct-Session-ID, or Framed-IP-Address attributes to identify the subscriber session. The CoA message also contains the Filter-Id attribute which specifies the name of the ACL with the **readdress server** rule. This enables applying the ACL dynamically to existing subscriber sessions. By default, the ACL is applied as both the input and output filter for the matching subscriber unless the Filter-Id in the CoA message bears the prefix **in:** or **out:**.

For information on CoA messages and how they are implemented in the system, refer to the [RADIUS Change of Authorization and Disconnect Message](#) section.



**Important:** Changing ACL and rulebase together in a single CoA is not supported. For this, two separate CoA requests can be sent through AAA server requesting for one attribute change per request.

## Session Limits On Redirection

To limit the amount of memory consumed by a session manager a limit of 2000 redirected session entries per session manager is allocated. This limit is equally shared by the set of subscribers who are currently being redirected. Whenever a redirected session entry is subject to revocation from a subscriber due to an insufficient number of available session entries, the least recently used entry is revoked.

## Stopping Redirection

The redirected session entries for a subscriber remain active until a CoA message issued from the RADIUS server specifies a filter that does not contain the readdress server ACL rule. When this happens, the redirected session entries for the subscriber are deleted.

All redirected session entries are also deleted when the subscriber disconnects.

## Handling IP Fragments

Since TCP/UDP port numbers are part of the redirection mechanism, fragmented IP datagrams must be reassembled before being redirected. Reassembly is particularly necessary when fragments are sent out of order. The session manager performs reassembly of datagrams and reassembly is attempted only when a datagram matches the redirect server ACL rule. To limit memory usage, only up to 10 different datagrams may be concurrently reassembled for a subscriber. Any additional requests cause the oldest datagram being reassembled to be discarded. The reassembly timeout is set to 2 seconds. In addition, the limit on the total number of fragments being reassembled by a session manager is set to 1000. If this limit is reached, the oldest datagram being reassembled in the session manager and its fragment list are discarded. These limits are not configurable.

## Recovery

When a session manager dies, the ACL rules are recovered. The session redirect entries have to be re-created when the MN initiates new traffic for the session. Therefore when a crash occurs, traffic from the Internet side is not redirected to the MN.

## AAA Accounting

Where destination-based accounting is implemented, traffic from the subscriber is accounted for using the original destination address and not the redirected address.

## Viewing the Redirected Session Entries for a Subscriber

View the redirected session entries for a subscriber by entering the following command:

```
show subscribers debug-info { callid <id> | msid <id> | username <name> }
```

The following command displays debug information for a subscriber with the MSID 0000012345:

```
show subscribers debug-info msid 0000012345
```

The following is a sample output of this command:

```
username: user1 callid: 01callb1 msid: 0000100003
```

## ■ Session Redirection (Hotlining)

Card/Cpu: 4/2

Sessmgr Instance: 7

Primary callline:

Redundancy Status: Original Session

Checkpoints Attempts Success Last-Attempt Last-Success

Full: 27 26 15700ms 15700ms

Micro: 76 76 4200ms 4200ms

Current state: SMGR\_STATE\_CONNECTED

FSM Event trace:

State Event

SMGR\_STATE\_OPEN SMGR\_EVT\_NEWCALL SMGR\_STATE\_NEWCALL\_ARRIVED SMGR\_EVT\_ANSWER\_CALL  
SMGR\_STATE\_NEWCALL\_ANSWERED SMGR\_EVT\_LINE\_CONNECTED SMGR\_STATE\_LINE\_CONNECTED  
SMGR\_EVT\_LINK\_CONTROL\_UP SMGR\_STATE\_LINE\_CONNECTED SMGR\_EVT\_AUTH\_REQ

SMGR\_STATE\_LINE\_CONNECTED SMGR\_EVT\_IPADDR\_ALLOC\_SUCCESS

SMGR\_STATE\_LINE\_CONNECTED SMGR\_EVT\_AUTH\_SUCCESS

SMGR\_STATE\_LINE\_CONNECTED SMGR\_EVT\_UPDATE\_SESS\_CONFIG

SMGR\_STATE\_LINE\_CONNECTED SMGR\_EVT\_LOWER\_LAYER\_UP

Data Reorder statistics

Total timer expiry: 0 Total flush (tmr expiry): 0

Total no buffers: 0 Total flush (no buffers): 0

Total flush (queue full): 0 Total flush (out of range): 0

Total flush (svc change): 0 Total out-of-seq pkt drop: 0

Total out-of-seq arrived: 0

IPv4 Reassembly Statistics:

Success: 0 In Progress: 0

Failure (timeout): 0 Failure (no buffers): 0

Failure (other reasons): 0

Redirected Session Entries:

Allowed: 2000 Current: 0

Added: 0 Deleted: 0

```
Revoked for use by different subscriber: 0

Peer callline:

Redundancy Status: Original Session

Checkpoints Attempts Success Last-Attempt Last-Success

Full: 0 0 0ms 0ms

Micro: 0 0 0ms 0ms

Current state: SMGR_STATE_CONNECTED

FSM Event trace:

State Event

SMGR_STATE_OPEN SMGR_EVT_MAKECALL

SMGR_STATE_MAKECALL_PENDING SMGR_EVT_LINE_CONNECTED

SMGR_STATE_LINE_CONNECTED SMGR_EVT_LOWER_LAYER_UP

SMGR_STATE_CONNECTED SMGR_EVT_AUTH_REQ

SMGR_STATE_CONNECTED SMGR_EVT_AUTH_SUCCESS

SMGR_STATE_CONNECTED SMGR_EVT_REQ_SUB_SESSION

SMGR_STATE_CONNECTED SMGR_EVT_RSP_SUB_SESSION

username: user1 callid: 01callb1 msid: 0000100003

Card/Cpu: 4/2

Sessmgr Instance: 7

Primary callline:

Redundancy Status: Original Session

Checkpoints Attempts Success Last-Attempt Last-Success

Full: 27 26 15700ms 15700ms

Micro: 76 76 4200ms 4200ms

Current state: SMGR_STATE_CONNECTED

FSM Event trace:

State Event

SMGR_STATE_OPEN SMGR_EVT_NEWCALL

SMGR_STATE_NEWCALL_ARRIVED SMGR_EVT_ANSWER_CALL
```

```

SMGR_STATE_NEWCALL_ANSWERED SMGR_EVT_LINE_CONNECTED

SMGR_STATE_LINE_CONNECTED SMGR_EVT_LINK_CONTROL_UP

SMGR_STATE_LINE_CONNECTED SMGR_EVT_AUTH_REQ

SMGR_STATE_LINE_CONNECTED SMGR_EVT_IPADDR_ALLOC_SUCCESS

SMGR_STATE_LINE_CONNECTED SMGR_EVT_AUTH_SUCCESS

SMGR_STATE_LINE_CONNECTED SMGR_EVT_UPDATE_SESS_CONFIG

SMGR_STATE_LINE_CONNECTED SMGR_EVT_LOWER_LAYER_UP

Data Reorder statistics

Total timer expiry: 0 Total flush (tmr expiry): 0

Total no buffers: 0 Total flush (no buffers): 0

Total flush (queue full): 0 Total flush (out of range):0

Total flush (svc change): 0 Total out-of-seq pkt drop: 0

    Total out-of-seq arrived: 0

IPv4 Reassembly Statistics:

Success: 0 In Progress: 0

Failure (timeout): 0 Failure (no buffers): 0

Failure (other reasons): 0

Redirected Session Entries:

Allowed: 2000 Current: 0

Added: 0 Deleted: 0

Revoked for use by different subscriber: 0

Peer callline:

Redundancy Status: Original Session

Checkpoints Attempts Success Last-Attempt Last-Success

Full: 0 0 0ms 0ms

Micro: 0 0 0ms 0ms

Current state: SMGR_STATE_CONNECTED

FSM Event trace:

State Event

```



```
SMGR_STATE_OPEN SMGR_EVT_MAKECALL
SMGR_STATE_MAKECALL_PENDING SMGR_EVT_LINE_CONNECTED
SMGR_STATE_LINE_CONNECTED SMGR_EVT_LOWER_LAYER_UP
SMGR_STATE_CONNECTED SMGR_EVT_AUTH_REQ
SMGR_STATE_CONNECTED SMGR_EVT_AUTH_SUCCESS
SMGR_STATE_CONNECTED SMGR_EVT_REQ_SUB_SESSION
SMGR_STATE_CONNECTED SMGR_EVT_RSP_SUB_SESSION
SMGR_STATE_CONNECTED SMGR_EVT_ADD_SUB_SESSION
SMGR_STATE_CONNECTED SMGR_EVT_AUTH_REQ
SMGR_STATE_CONNECTED SMGR_EVT_AUTH_SUCCESS

Data Reorder statistics

Total timer expiry: 0 Total flush (tmr expiry): 0
Total no buffers: 0 Total flush (no buffers): 0
Total flush (queue full): 0 Total flush (out of range):0
Total flush (svc change): 0 Total out-of-seq pkt drop: 0
Total out-of-seq arrived: 0

IPv4 Reassembly Statistics:

Success: 0 In Progress: 0

Failure (timeout): 0 Failure (no buffers): 0
Failure (other reasons): 0

Redirected Session Entries:

Allowed: 2000 Current: 0

Added: 0 Deleted: 0

Revoked for use by different subscriber: 0
```




# Appendix B


## GRE Protocol Interface

---

This chapter provides information on Generic Routing Encapsulation protocol interface support in the GGSN or P-GW service node. The product Administration Guides provide examples and procedures for configuration of basic services on the system. It is recommended that you select the configuration example that best meets your service model, and configure the required elements for that model, as described in the respective product Administration Guide, before using the procedures in this chapter.

---

 **Important:** GRE protocol interface support is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

 **Important:** Commands used in the configuration samples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the *Command Line Interface Reference* for complete information regarding all commands.

---

This chapter discusses following topics for GRE protocol interface support:

- [Introduction](#)
- [Supported Standards](#)
- [Supported Networks and Platforms](#)
- [Services and Application on GRE Interface](#)
- [How GRE Interface Support Works](#)
- [GRE Interface Configuration](#)
- [Verifying Your Configuration](#)

# Introduction

GRE protocol functionality adds one additional protocol on Cisco's multimedia core platforms (ASR 5000 or higher) to support mobile users to connect to their enterprise networks through Generic Routing Encapsulation (GRE).

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

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

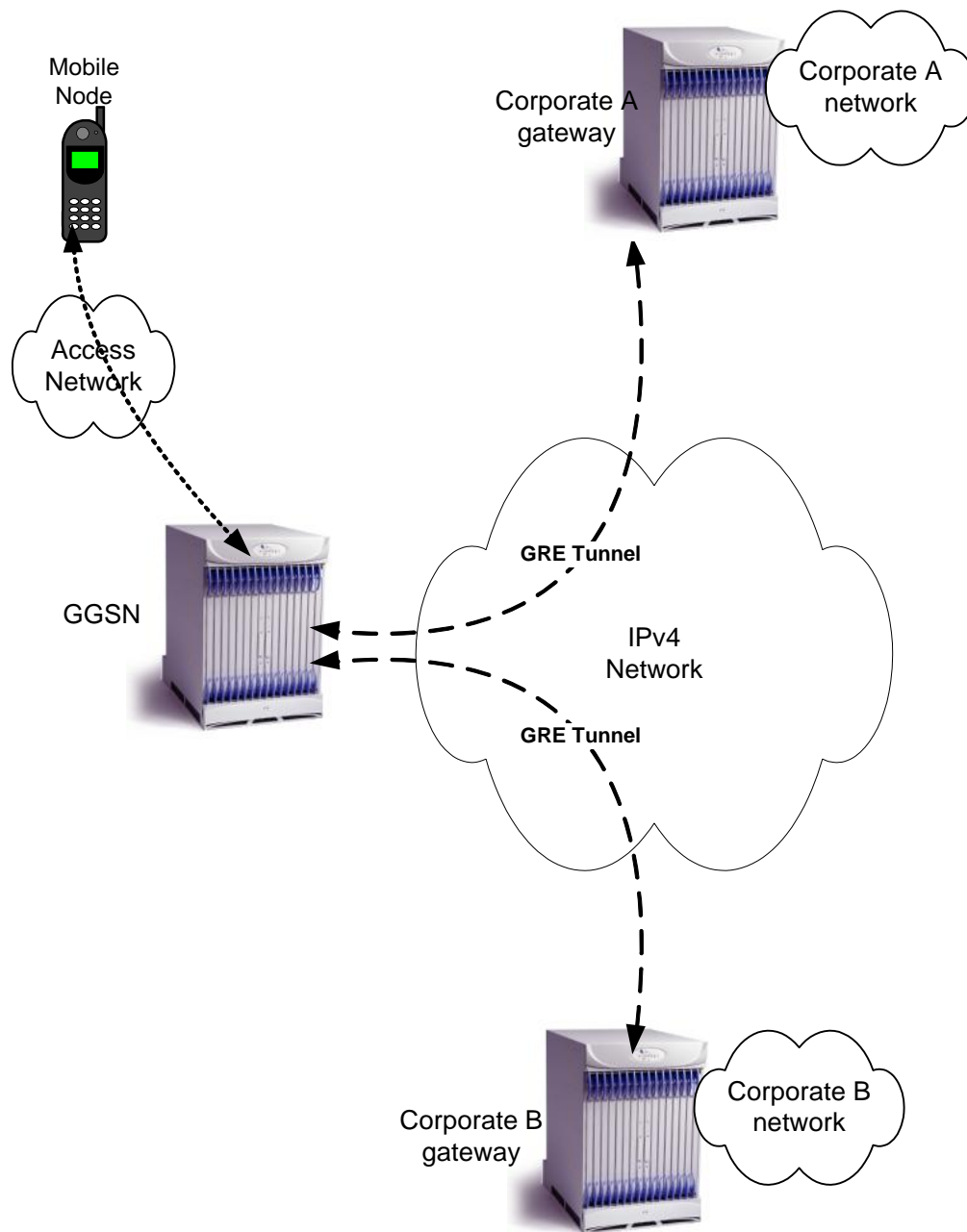
It is a common technique to enable multi-protocol local networks over a single-protocol backbone, to connect non-contiguous networks and allow virtual private networks across WANs. This mechanism encapsulates data packets from one protocol inside a different protocol and transports the data packets unchanged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

GRE Tunneling consists of three main components:

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

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

Figure 35. GRE Interface Deployment Scenario



## Supported Standards

Support for the following standards and requests for comments (RFCs) have been added with this interface support:

- RFC 1701, Generic Routing Encapsulation (GRE)
- RFC 1702, Generic Routing Encapsulation over IPv4 networks
- RFC 2784, Generic Routing Encapsulation (GRE)
- RFC 2890, Key and Sequence Number Extensions to GRE

## Supported Networks and Platforms

This feature supports all systems with StarOS Release 9.0 or later running GGSN and/or SGSN service for the core network services. The P-GW service supports this feature with StarOS Release 12.0 or later.

## Licenses

GRE protocol interface support is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.



## Services and Application on GRE Interface

GRE interface implementation provides the following functionality with GRE protocol support.

## How GRE Interface Support Works

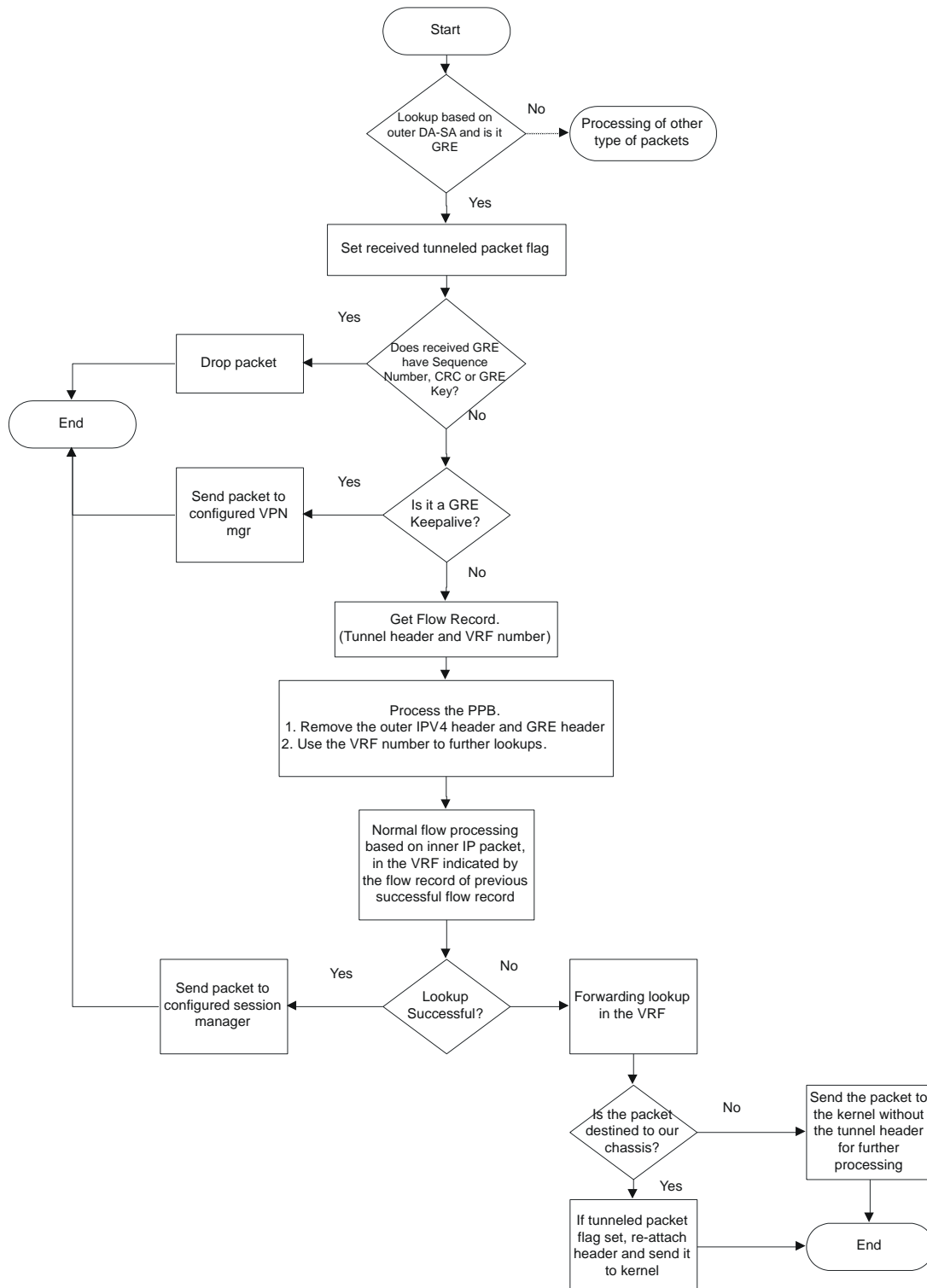
The GRE interface provides two types of data processing; one for ingress packets and another for egress packets.

### Ingress Packet Processing on GRE Interface

Figure given below provides a flow of process for incoming packets on GRE interface.

Note that in case the received packet is a GRE keep-alive or a ping packet then the outer IPV4 and GRE header are not stripped off (or get reattached), but instead the packet is forwarded as is to the VPN manager or kernel respectively. In case of all other GRE tunneled packets the IPV4 and GRE header are stripped off before sending the packet for a new flow lookup.

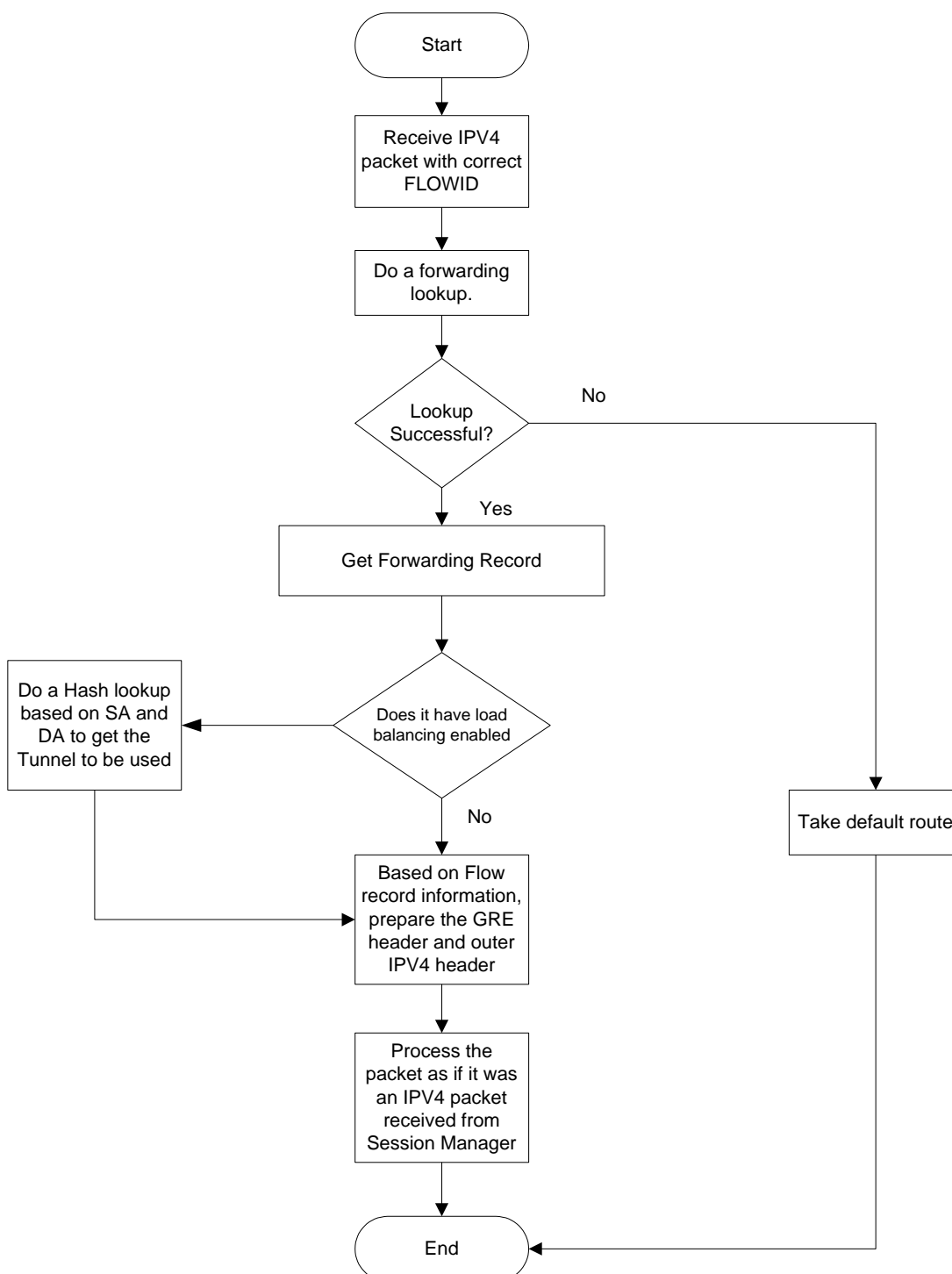
Figure 36. Ingress Packet Processing on GRE Interface



## Egress Packet Processing on GRE Interface

Figure given below provides a flow of process for outgoing packets on GRE interface:

Figure 37. Egress Packet Processing on GRE Interface



# GRE Interface Configuration

This section provides a high-level series of steps and the associated configuration examples for configuring the system with GRE interface in GGSN or P-GW services.



**Important:** This section provides the minimum instruction set to enable the GRE Protocol Interface support functionality on a GGSN or P-GW. Commands that configure additional functions for this feature are provided in the *Command Line Interface Reference*.

These instructions assume that you have already configured the system level configuration as described in *System Administration Guide* and specific product Administration Guide.

To configure the system to support GRE tunnel interface:

- Step 1** Configure the virtual routing and forwarding (VRF) in a context by applying the example configurations presented in the [Virtual Routing And Forwarding \(VRF\) Configuration](#) section.
- Step 2** Configure the GRE tunnel interface in a context by applying the example configurations presented in the [GRE Tunnel Interface Configuration](#) section.
- Step 3** Enable OSPF for the VRF and for the given network by applying the example configurations presented in the [Enabling OSPF for VRF](#) section.
- Step 4** Associate IP pool and AAA server group with VRF by applying the example configurations presented in the [Associating IP Pool and AAA Group with VRF](#) section.
- Step 5** Associate APN with VRF through AAA server group and IP pool by applying the example configurations presented in the [Associating APN with VRF](#) section.
- Step 6** Optional. If the route to the server is not learnt from the corporate over OSPFv2, static route can be configured by applying the example configurations presented in the [Static Route Configuration](#) section.
- Step 7** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.
- Step 8** Verify configuration of GRE and VRF related parameters by applying the commands provided in the *Verifying Your Configuration* section of this chapter.

## Virtual Routing And Forwarding (VRF) Configuration

This section provides the configuration example to configure the VRF in a context:

```
configure

context <vpn_context_name> -noconfirm ]

    ip vrf <vrf_name>

        ip maximum-routes <max_routes>
```

```
end
```

#### Notes:

- `<vpn_context_name>` is the name of the system context you want to use for VRF. For more information, refer *System Administration Guide*.
- A maximum of 100 VRFs in one context and up to 1024 VRFs on one chassis can be configured on system.
- `<vrf_name>` is name of the VRF which is to be associated with various interfaces.
- A maximum of 10000 routes can be configured through `ip maximum-routes <max_routes>` command.

## GRE Tunnel Interface Configuration

This section provides the configuration example to configure the GRE tunnel interface and associate a VRF with GRE interface:

```
configure
```

```
context <vpn_context_name>

ip interface <intfc_name> tunnel

ip vrf forwarding <vrf_name>

ip address <internal_ip_address/mask>

tunnel-mode gre

source interface <non_tunn_intfc_to_corp>

destination address <global_ip_address>

keepalive interval <value> num-retry <retry>

end
```

#### Notes:

- `<vpn_context_name>` is the name of the system context you want to use for GRE interface configuration. For more information, refer *Command Line Interface Reference*.
- A maximum of 511 GRE tunnels + 1 non-tunnel interface can be configured in one context. System needs at least 1 non-tunnel interface as a default.
- `<intfc_name>` is name of the IP interface which is defined as a tunnel type interface and to be used for GRE tunnel interface.
- `<vrf_name>` is the name of the VRF which is preconfigured in context configuration mode.
- `<internal_ip_address/mask>` is the network IP address with sub-net mask to be used for VRF forwarding.
- `<non_tunn_intfc_to_corp>` is the name a non-tunnel interface which is required by system as source interface and preconfigured. For more information on interface configuration refer *System Administration Guide*.
- `<global_ip_address>` is a globally reachable IP address to be used as a destination address.

## Enabling OSPF for VRF

This section provides the configuration example to enable the OSPF for VRF to support GRE tunnel interface:

```
configure

context <vpn_context_name>

    router ospf

        ip vrf <vrf_name>

        network <internal_ip_address/mask>

    end
```

Notes:

- <vpn\_context\_name> is the name of the system context you want to use for OSPF routing. For more information, refer *Routing* in this guide.
- <vrf\_name> is the name of the VRF which is preconfigured in context configuration mode.
- <internal\_ip\_address/mask> is the network IP address with sub-net mask to be used for OSPF routing.

## Associating IP Pool and AAA Group with VRF

This section provides the configuration example for associating IP pool and AAA groups with VRF:

```
configure

context <vpn_context_name>

    ip pool <ip_pool_name> <internal_ip_address/mask> vrf <vrf_name>

    exit

    aaa group <aaa_server_group>

        ip vrf <vrf_name>

    end
```

Notes:

- <vpn\_context\_name> is the name of the system context you want to use for IP pool and AAA server group.
- <ip\_pool\_name> is name of a preconfigured IP pool. For more information refer *System Administration Guide*.
- <aaa\_server\_group> is name of a preconfigured AAA server group. For more information refer *AAA Interface Administration and Reference*.
- <vrf\_name> is the name of the VRF which is preconfigured in context configuration mode.
- <internal\_ip\_address/mask> is the network IP address with sub-net mask to be used for IP pool.

## Associating APN with VRF

This section provides the configuration example for associating an APN with VRF through AAA group and IP pool:

```
configure

context <vpn_context_name>

  apn <apn_name>

  aaa group <aaa_server_group>

  ip address pool name <ip_pool_name>

end
```

Notes:

- <vpn\_context\_name> is the name of the system context you want to use for APN configuration.
- <ip\_pool\_name> is name of a preconfigured IP pool. For more information refer *System Administration Guide*.
- <aaa\_server\_group> is name of a preconfigured AAA server group. For more information refer *AAA Interface Administration and Reference*.
- <vrf\_name> is the name of the VRF which is preconfigured in context configuration mode.

## Static Route Configuration

This section provides the optional configuration example for configuring static routes when the route to the server is not learnt from the corporate over OSPFv2:

```
configure

context <vpn_context_name>

  ip route <internal_ip_address/mask> tunnel <tunnel_intf_name> vrf <vrf_name>

end
```

Notes:


- <vpn\_context\_name> is the name of the system context you want to use for static route configuration.
- <internal\_ip\_address/mask> is the network IP address with sub-net mask to be used as static route.
- <tunnel\_intf\_name> is name of a predefined tunnel type IP interface which is to be used for GRE tunnel interface.
- <vrf\_name> is the name of the VRF which is preconfigured in context configuration mode.



## Verifying Your Configuration

This section explains how to display and review the configurations after saving them in a .cfg file as described in the *System Administration Guide* and also to retrieve errors and warnings within an active configuration for a service.

---

 **Important:** All commands listed here are under Exec mode. Not all commands are available on all platforms.

---

These instructions are used to verify the GRE interface configuration.

**Step 1** Verify that your interfaces are configured properly by entering the following command in Exec Mode:

**show ip interface**

The output of this command displays the configuration of the all interfaces configured in a context.

```

Intf Name:      fool

Intf Type:      Broadcast

Description:

IP State:       UP (Bound to 17/2 untagged, ifIndex 285343745)

IP Address:     1.1.1.1          Subnet Mask:      255.255.255.0

Bcast Address:  1.1.1.255       MTU:              1500

Resoln Type:    ARP             ARP timeout:      60 secs

L3 monitor LC-port switchover: Disabled

Number of Secondary Addresses: 0

Intf Name:      foo2

Intf Type:      Tunnel (GRE)

Description:

VRF:            vrf-tun

IP State:       UP (Bound to local address 1.1.1.1 (fool), remote
address 5.5.5.5)

IP Address:     10.1.1.1         Subnet Mask:      255.255.255.0

Intf Name:      foo3

Intf Type:      Tunnel (GRE)

Description:

IP State:       DOWN (<state explaining the reason of being down>)
```

## ■ Verifying Your Configuration

IP Address: 20.20.20.1 Subnet Mask: 255.255.255.0

**Step 2** Verify that GRE keep alive is configured properly by entering the following command in Exec Mode:

```
show ip interface gre-keepalive
```

The output of this command displays the configuration of the keepalive for GRE interface configured in a context.

# Appendix C

## Gx Interface Support

---

This chapter provides information on configuring Gx interface to support policy and charging control for subscribers.

The IMS service provides application support for transport of voice, video, and data independent of access support. Roaming IMS subscribers require apart from other functionality sufficient, uninterrupted, consistent, and seamless user experience during an application session. It is also important that a subscriber gets charged only for the resources consumed by the particular IMS application used.

It is recommended that before using the procedures in this chapter you select the configuration example that best meets your service model, and configure the required elements for that model as described in this Administration Guide.

The following topics are covered in this chapter:

- [Rel. 6 Gx Interface](#)
- [Rel. 7 Gx Interface](#)
- [Rel. 8 Gx Interface](#)
- [Rel. 9 Gx Interface](#)

## Rel. 6 Gx Interface

Rel. 6 Gx interface support is available on the Cisco ASR chassis running StarOS 8.0 and later releases for the following products:

- GGSN
- IPSG

This section describes the following topics:

- [Introduction](#)
- [How it Works](#)
- [Configuring Rel. 6 Gx Interface](#)

### Introduction

In GPRS/UMTS networks, the client functionality lies with the GGSN/IPSG, therefore in the IMS authorization scenario it is also called Access Gateway (AGW).

The provisioning of charging rules that are based on the dynamic analysis of flows used for the IMS session is carried out over the Gx interface. In 3GPP, Rel. 6 the Gx is an interface between Access Gateway functioning as Traffic Plane Function (TPF) and the Charging Rule Function (CRF). It is based on the Diameter Base Protocol (DIABASE) and the Diameter Credit Control Application (DCCA) standard. The GGSN/TPF acts as the client where as the CRF contains the Diameter server functionality.

The AGW is required to perform query, in reply to which the servers provision certain policy or rules that are enforced at the AGW for that particular subscriber session. The CRF analyzes the IP flow data, which in turn has been retrieved from the Session Description Protocol (SDP) data exchanged during IMS session establishment.



**Important:** In addition to standard Gx interface functionality, the Gx interface implemented here provides support of SBLP with additional AVPs in custom DPCA dictionaries. For more information on customer-specific support contact your local technical support representative. In view of required flow bandwidth and QoS, the system provides enhanced support for use of Service Based Local Policy (SBLP) to provision and control the resources used by the IMS subscriber. SBLP is based on the dynamic parameters such as the media/traffic flows for data transport, network conditions and static parameters, such as subscriber configuration and category. It also provides Flow-based Charging (FBC) mechanism to charge the subscriber dynamically based on content usage. With this additional functionality, the Cisco Systems Gateway can act as an Enhanced Policy Decision Function (E-PDF).

### Supported Networks and Platforms

This feature is supported on all chassis with StarOS Release 8.0 or later running GGSN service for the core network services.

### License Requirements

The Rel. 6 Gx interface support is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing

and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

## Supported Standards

The Rel 6. Gx interface support is based on the following standards and request for comments (RFCs):

- 3GPP TS 29.210, Charging rule provisioning over Gx interface
- RFC 3588, Diameter Base Protocol; September 2003
- RFC 4006, Diameter Credit-Control Application; August 2005

In addition to the above RFCs and standards, IMS Authorization partially supports 3GPP TS 29.212 for Policy and Charging Control over Gx reference point functionality.

## How it Works

This section describes the IMS authorization and dynamic policy support in GPRS/UMTS networks.

The following figure and table explain the IMS authorization process between a system and IMS components that is initiated by the MN.

In the case of GGSN, the DPCA is the Gx interface to the Control and Charging Rule Function (CRF). In this context CRF will act as Enhanced Policy Decision Function (E-PDF). The CRF may reside in Proxy-Call Session Control Function (P-CSCF) or on stand-alone system.

The interface between IMSA with CRF is the Gx interface, and between Session Manager and Online Charging Service (OCS) is the Gy interface.

Note that the IMS Authorization (IMSA) service and Diameter Policy Control Application (DPCA) are part of Session Manager on the system, and separated in the following figure for illustration purpose only.

Figure 38. Rel. 6 Gx IMS Authorization Call Flow

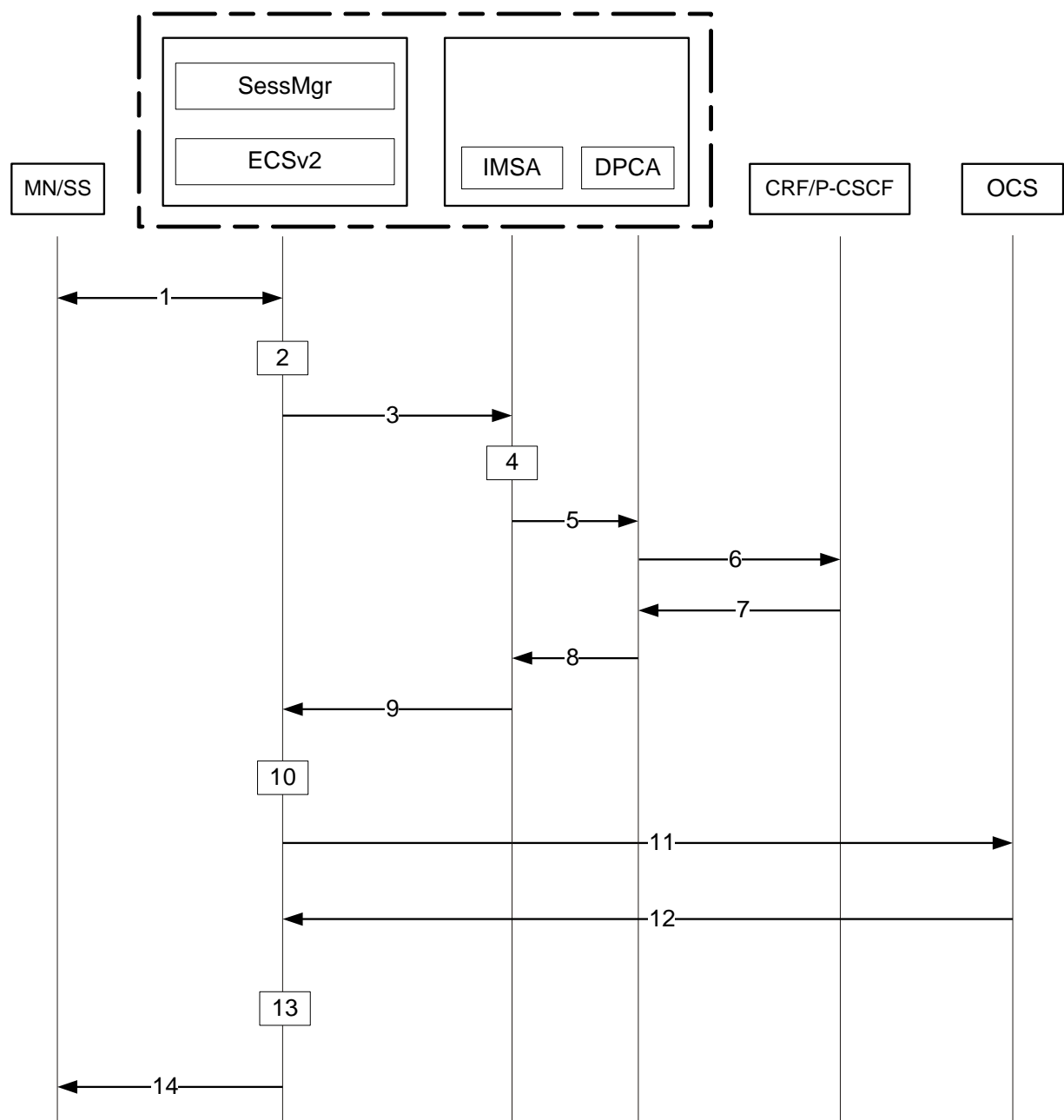


Table 16. Rel. 6 Gx IMS Authorization Call flow Description

Step	Description
1	IMS subscriber (MN) sends request for primary PDP context activation/creation.
2	Session manager allocates IP address to MN.

Step	Description
3	Session manager sends IMS authorization request to IMS Authorization service (IMSA).
4	IMSA creates a session with the CRF on the basis of CRF configuration.
5	IMSA sends request to DPCA module to issue the authorization request to selected CRF.
6	DPCA sends a CCR-initial message to the selected CRF. This message includes the IP address allocated to MN.
7	CCA message sent to DPCA. If a preconfigured rule set for the PDP context is provided in CRF, it sends that charging rules to DPCA in CCA message.
8	DPCA module calls the callback function registered with it by IMSA.
9	After processing the charging rules, IMSA sends Policy Authorization Complete message to session manager.
10	The rules received in CCA message are used for dynamic rule configuration structure and session manager sends the message to ECS.
11	ECS installs the rules and performs credit authorization by sending CCR-Initial to Online Charging System (OCS) with CC-Request-Type set to INITIAL_REQUEST to open the credit control session. This request includes the active rule base ID and 3GPP specific attributes (for example, APN, QoS and so on).
12	OCS returns a CCA-Initial message to activate the statically configured rulebase and includes preemptive credit quotas.
13	ECS responds to session manager with the response message for dynamic rule configuration.
14	On the basis of response for the PDP context authorization, Session Manager sends the response to the MN and activates/rejects the call.

## Configuring Rel. 6 Gx Interface

To configure Rel. 6 Gx interface functionality:

- Step 1** Configure the IMS Authorization Service at the context level for an IMS subscriber in GPRS/UMTS network as described in the [Configuring IMS Authorization Service at Context Level](#) section.
- Step 2** Verify your configuration, as described in the [Verifying IMS Authorization Service Configuration](#) section.
- Step 3** Configure an APN within the same context to use the IMS Authorization service for an IMS subscriber as described in the [Applying IMS Authorization Service to an APN](#) section.
- Step 4** Verify your configuration as described in the [Verifying Subscriber Configuration](#) section.
- Step 5** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.



**Important:** Commands used in the configuration examples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the *Command Line Interface Reference* for complete information regarding all commands.

## Configuring IMS Authorization Service at Context Level

Use the following example to configure IMS Authorization Service at context level for IMS subscribers in GPRS/UMTS networks:

```
configure

context <context_name>

    ims-auth-service <imsa_service_name>

        p-cscf table { 1 | 2 } row-precedence <precedence_value> { address <ip_address>
| ipv6-address <ipv6_address> }

        p-cscf discovery { table { 1 | 2 } [ algorithm { ip-address-modulus | msisd-
modulus | round-robin } ] | diameter-configured }

        policy-control

            diameter origin endpoint <endpoint_name>

            diameter dictionary <dictionary>

            failure-handling cc-request-type { any-request | initial-request | terminate-
request | update-request } { diameter-result-code { any-error | <result_code> [ to
<end_result_code> ] } } { continue | retry-and-terminate | terminate }

            diameter host-select row-precedence <precedence_value> table { 1 | 2 } host
<host_name> [ realm <realm_name> ] [ secondary host <host_name> [ realm <realm_name> ] ]

            diameter host-select reselect subscriber-limit <subscriber_limit> time-
interval <duration>

            diameter host-select table { 1 | 2 } algorithm { ip-address-modulus | msisd-
modulus | round-robin }

        end
```

Notes:

- <context\_name> must be the name of the context where you want to enable IMS Authorization Service.
- <imsa\_service\_name> must be the name of the IMS Authorization Service to be configured for the Gx interface authentication.
- A maximum of 16 authorization services can be configured globally in a system. There is also a system limit for maximum number of total configured services.
- Secondary P-CSCF IP address can be configured in the P-CSCF table. Refer to the *Command Line Interface Reference* for more information on the **p-cscf table** command.
- To enable Rel. 6 Gx interface support, specific Diameter dictionary must be configured. For information on the Diameter dictionary to use, please contact your local service representative.
- *Optional:* To configure the quality of service (QoS) update timeout for a subscriber, in the IMS Authorization Service Configuration Mode, enter the following command:

```
qos-update-timeout <timeout_duration>
```



- *Optional:* To configure signalling restrictions, in the IMS Authorization Service Configuration Mode, enter the following commands:  

```
signaling-flag { deny | permit }

signaling-flow permit server-address <ip_address> [ server-port { <port_number> |
range <start_number> to <end_number> } ] [ description <string> ]
```
- *Optional:* To configure action on packets that do not match any policy gates in the general purpose PDP context, in the IMS Authorization Service Configuration Mode, enter the following command:  

```
traffic-policy general-pdp-context no-matching-gates direction { downlink | uplink
} { forward | discard }
```
- *Optional:* To configure the algorithm to select Diameter host table, in the Policy Control Configuration Mode, enter the following command:  

```
diameter host-select table { 1 | 2 } algorithm { ip-address-modulus | msisd-
modulus | round-robin }
```

## Verifying IMS Authorization Service Configuration

To verify the IMS Authorization Service configuration:

- Step 1** Change to the context where you enabled IMS Authorization Service by entering the following command:

```
context <context_name>
```

- Step 2** Verify the IMS Authorization Service's configurations by entering the following command:

```
show ims-authorization service name <imsa_service_name>
```

## Applying IMS Authorization Service to an APN

After configuring IMS Authorization service at the context-level, an APN within the same context must be configured to use the IMS Authorization service for an IMS subscriber.

Use the following example to apply IMS Authorization service functionality to a previously configured APN within the context configured in the Configuring IMS Authorization Service section.

**configure**

```
context <context_name>

apn <apn_name>

ims-auth-service <imsa_service_name>

end
```

Notes:

- <context\_name> must be the name of the context in which the IMS Authorization service was configured.
- <imsa\_service\_name> must be the name of the IMS Authorization Service configured for IMS authentication in the context.

## Verifying Subscriber Configuration

Verify the IMS Authorization Service configuration for subscriber(s) by entering the following command:

```
show subscribers ims-auth-service <imsa_service_name>
```

<imsa\_service\_name> must be the name of the IMS Authorization Service configured for IMS authentication.

# Rel. 7 Gx Interface

Rel. 7 Gx interface support is available on the Cisco ASR chassis running StarOS 8.1 or StarOS 9.0 and later releases for the following products:

- GGSN
- IPSG

This section describes the following topics:

- [Introduction](#)
- [Terminology and Definitions](#)
- [How it Works](#)
- [Configuring Rel. 7 Gx Interface](#)
- [Gathering Statistics](#)

## Introduction

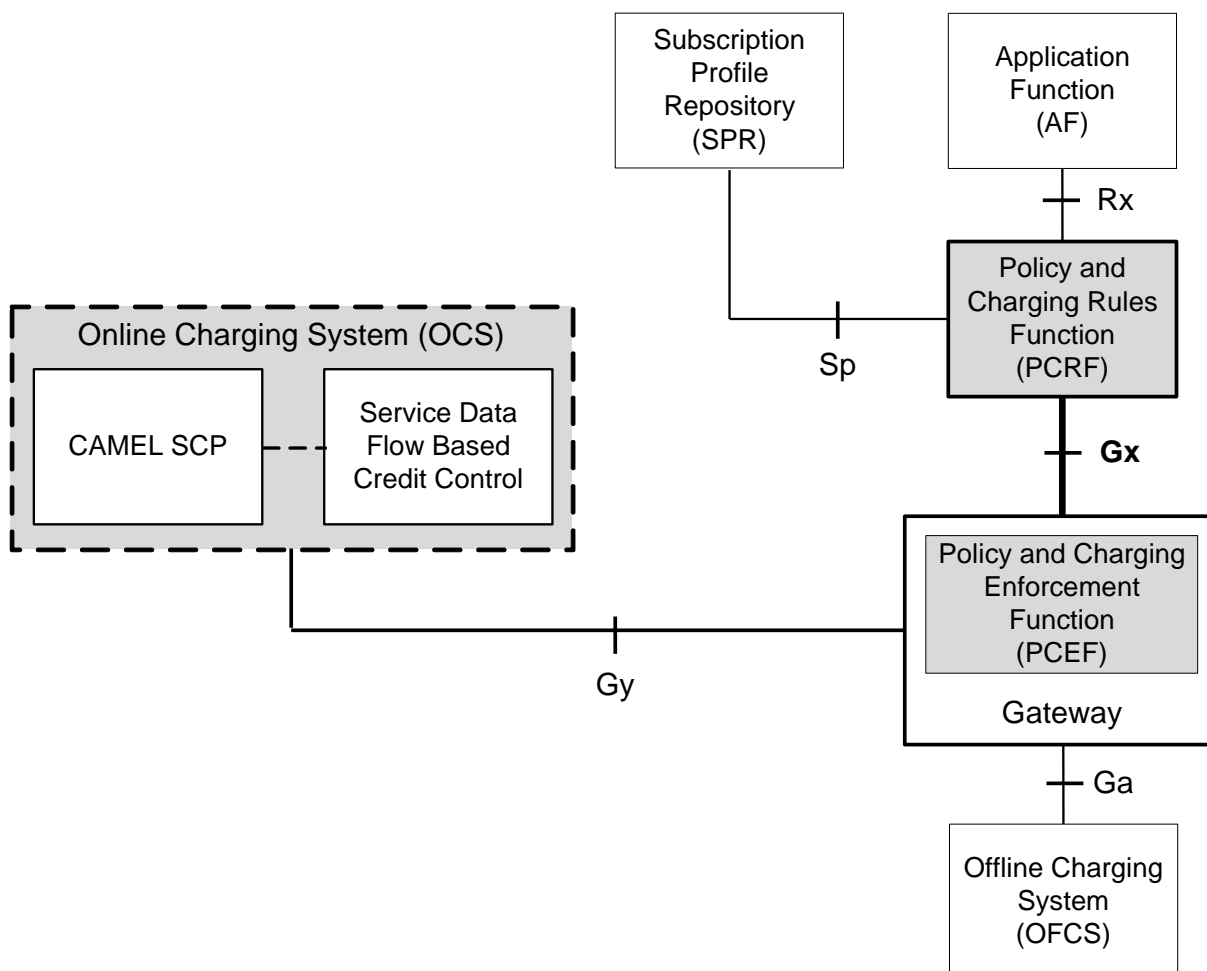
For IMS deployment in GPRS/UMTS networks the system uses Rel. 7 Gx interface for policy-based admission control support and flow-based charging. The Rel. 7 Gx interface supports enforcing policy control features like gating, bandwidth limiting, and so on, and also supports flow-based charging. This is accomplished via dynamically provisioned Policy Control and Charging (PCC) rules. These PCC rules are used to identify Service Data Flows (SDF) 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)/Cisco Systems GGSN and the Policy and Charging Rules Function (PCRF).

In GPRS/UMTS networks, the client functionality lies with the GGSN, therefore in the IMS authorization scenario it is also called the Gateway. In the following figure, Gateway is the Cisco Systems GGSN, and the PCEF function is provided by Enhanced Charging Service (ECS). The Rel 7. Gx interface is implemented as a Diameter connection. The Gx messages mostly involve installing/modifying/removing dynamic rules and activating/deactivating predefined rules.

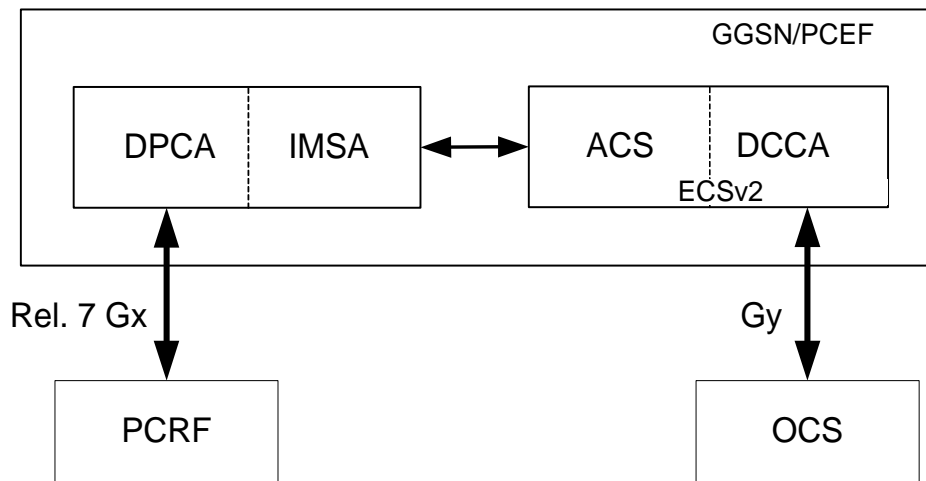
The Rel. 7 Gx reference point is located between the Gateway and the PCRF. This reference point is used for provisioning and removal of PCC rules from the PCRF to the Gateway, and the transmission of traffic plane events from the Gateway to the PCRF. The Gx reference point can be used for charging control, policy control, or both by applying AVPs relevant to the application. The following figure shows the reference points between various elements involved in the policy and charging architecture.

Figure 39. PCC Logical Architecture



Within the Gateway, the IMSA and DPCA modules handle the Gx protocol related functions (at the SessMgr) and the policy enforcement and charging happens at ECS. The Gy protocol related functions are handled within the DCCA module (at the ECS). The following figure shows the interaction between components within the Gateway.

Figure 40. PCC Architecture within Cisco PCEF



## Supported Networks and Platforms

This feature is supported on all chassis with StarOS Release 8.1 and later running GGSN service for the core network services.

## License Requirements

The Rel. 7 Gx interface support is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

## Supported Standards

The Rel 7. Gx interface support is based on the following standards and RFCs:

- 3GPP TS 23.203 V7.6.0 (2008-03): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Policy and charging control architecture (Release 7)
- 3GPP TS 29.212 V7.8.0 (2009-03): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control over Gx reference point (Release 7)
- 3GPP TS 29.213 V7.4.0 (2008-03): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control signalling flows and QoS parameter mapping; (Release 7)
- RFC 3588, Diameter Base Protocol; September 2003
- RFC 4006, Diameter Credit-Control Application; August 2005

## Terminology and Definitions

This section describes features and terminology pertaining to Rel. 7 Gx functionality.

### Policy Control

The process whereby the PCRF indicates to the PCEF how to control the IP-CAN bearer.

Policy control comprises the following functions:

- **Binding:** Binding is the generation of an association between a Service Data Flow (SDF) and the IP CAN bearer (for GPRS a PDP context) transporting that SDF.

The QoS demand in the PCC rule, as well as the SDF template are input for the bearer binding. The selected bearer will have the same QoS Class as the one indicated by the PCC rule.

Depending on the type of IP-CAN and bearer control mode, bearer binding can be executed either by the PCRF, or both PCRF and PCEF.

- For UE-only IP-CAN bearer establishment mode, the PCRF performs bearer binding. When the PCRF performs bearer binding, it indicates the bearer (PDP context) by means of Bearer ID. The Bearer ID uniquely identifies the bearer within the PDP session.
  - For UE/NW IP-CAN bearer establishment mode, the PCRF performs the binding of the PCC rules for user controlled services, while the PCEF performs the binding of the PCC rules for the network-controlled services.
- **Gating Control:** Gating control is the blocking or allowing of packets, belonging to an SDF, to pass through to the desired endpoint. A gate is described within a PCC rule and gating control is applied on a per SDF basis. The commands to open or close the gate leads to the enabling or disabling of the passage for corresponding IP packets. If the gate is closed, all packets of the related IP flows are dropped. If the gate is opened, the packets of the related IP flows are allowed to be forwarded.
- **Event Reporting:** Event reporting is the notification of and reaction to application events to trigger new behavior in the user plane as well as the reporting of events related to the resources in the Gateway (PCEF).
  - Event triggers may be used to determine which IP-CAN session modification or specific event causes the PCEF to re-request PCC rules. Although event trigger reporting from PCEF to PCRF can apply for an IP CAN session or bearer depending on the particular event, provisioning of event triggers will be done at session level.

Note that in 11.0 and later releases, RAR with unknown event triggers are silently ignored and responded with DIAMETER\_SUCCESS. In earlier releases, when unknown event triggers were received in the RAR command from PCRF, invalid AVP result code was set in the RAA command.

- The Event Reporting Function (ERF) receives event triggers from PCRF during the Provision of PCC Rules procedure and performs event trigger detection. When an event matching the received event trigger occurs, the ERF reports the occurred event to the PCRF. If the provided event triggers are associated with certain parameter values then the ERF includes those values in the response back to the PCRF. The Event Reporting Function is located in the PCEF.



**Important:** In this release, event triggers “IP-CAN\_CHANGE” and “MAX\_NR\_BEARERS\_REACHED” are not supported.

- **QoS Control:** QoS control is the authorization and enforcement of the maximum QoS that is authorized for a SDF or an IP-CAN bearer or a QoS Class Identifier (QCI). In case of an aggregation of multiple SDFs (for

GPRS a PDP context), the combination of the authorized QoS information of the individual SDFs is provided as the authorized QoS for this aggregate.

- QoS control per SDF allows the PCC architecture to provide the PCEF with the authorized QoS to be enforced for each specific SDF.
- The enforcement of the authorized QoS of the IP-CAN bearer may lead to a downgrading or upgrading of the requested bearer QoS by the Gateway (PCEF) as part of a UE-initiated IP-CAN bearer establishment or modification. Alternatively, the enforcement of the authorized QoS may, depending on operator policy and network capabilities, lead to network-initiated IP-CAN bearer establishment or modification. If the PCRF provides authorized QoS for both, the IP-CAN bearer and PCC rule(s), the enforcement of authorized QoS of the individual PCC rules takes place first.
- QoS authorization information may be dynamically provisioned by the PCRF, or it can be a predefined PCC rule in the PCEF. In case the PCRF provides PCC rules dynamically, authorized QoS information for the IP-CAN bearer (combined QoS) may be provided. For a predefined PCC rule within the PCEF, the authorized QoS information takes affect when the PCC rule is activated. The PCEF combines the different sets of authorized QoS information, that is the information received from the PCRF and the information corresponding to the predefined PCC rules. The PCRF knows the authorized QoS information of the predefined PCC rules and takes this information into account when activating them. This ensures that the combined authorized QoS of a set of PCC rules that are activated by the PCRF is within the limitations given by the subscription and operator policies regardless of whether these PCC rules are dynamically provided, predefined, or both.



**Important:** In this release, QoS Resource Reservation is not supported.

#### Supported Features:

- Provisioning and Policy Enforcement of Authorized QoS: The PCRF may provide authorized QoS to the PCEF. The authorized QoS provides appropriate values for resources to be enforced.
- Provisioning of “Authorized QoS” Per IP CAN Bearer: The authorized QoS per IP-CAN bearer is used if the bearer binding is performed by the PCRF.
- Policy Enforcement for “Authorized QoS” per IP CAN Bearer: The PCEF is responsible for enforcing the policy-based authorization, that is to ensure that the requested QoS is in-line with the “Authorized QoS” per IP CAN Bearer.
- Policy Provisioning for Authorized QoS Per SDF: The provisioning of authorized QoS per SDF is a part of PCC rule provisioning procedure.
  - Policy Enforcement for Authorized QoS Per SDF: If an authorized QoS is defined for a PCC rule, the PCEF limits the data rate of the SDF corresponding to that PCC rule not to exceed the maximum authorized bandwidth for the PCC rule by discarding packets exceeding the limit.
  - Upon deactivation or removal of a PCC rule, the PCEF frees the resources reserved for that PCC rule. If the PCRF provides authorized QoS for both the IP-CAN bearer and PCC rule(s), the enforcement of authorized QoS of the individual PCC rules takes place first.



**Important:** In this release, coordination of authorized QoS scopes in mixed mode (BCM = UE\_NW) is not supported.

- Provisioning of Authorized QoS Per QCI: If the PCEF performs the bearer binding, the PCRF may provision an authorized QoS per QCI for non-GBR bearer QCI values. If the PCRF performs the

bearer binding the PCRF does not provision an authorized QoS per QCI. The PCRF does not provision an authorized QoS per QCI for GBR bearer QCI values.

- Policy Enforcement for Authorized QoS per QCI: The PCEF can receive an authorized QoS per QCI for non GBR-bearer QCI values.
- Other Features:
  - Bearer Control Mode Selection: The PCEF may indicate, via the Gx reference point, a request for Bearer Control Mode (BCM) selection at IP-CAN session establishment or IP-CAN session modification (as a consequence of an SGSN change). It will be done using the “PCC Rule Request” procedure.

If the Bearer-Control-Mode AVP is not received from PCRF, the IP-CAN session is not terminated. The value negotiated between UE/SGSN/GGSN is considered as the BCM. The following values are considered for each of the service types:

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

In the following scenarios UE\_ONLY is chosen as the BCM:

Scenario 1:

- UE-> UE\_ONLY
- SGSN-> UE\_ONLY
- GGSN-> UE\_ONLY
- PCRF-> NO BCM

Scenario 2:

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

- PCC Rule Error Handling: If the installation/activation of one or more PCC rules fails, the PCEF includes one or more Charging-Rule-Report AVP(s) in either a CCR or an RAA command for the affected PCC rules. Within each Charging-Rule-Report AVP, the PCEF identifies the failed PCC rule(s) by including the Charging-Rule-Name AVP(s) or Charging-Rule-Base-Name AVP(s), identifies the failed reason code by including a Rule-Failure-Code AVP, and includes the PCC-Rule-Status AVP.

If the installation/activation of one or more new PCC rules (that is, rules that were not previously successfully installed) fails, the PCEF sets the PCC-Rule-Status to INACTIVE for both the PUSH and the PULL modes.

If a PCC rule was successfully installed/activated, but can no longer be enforced by the PCEF, the PCEF shall send the PCRF a new CCR command and include a Charging-Rule-Report AVP. The PCEF shall include the Rule-Failure-Code AVP within the Charging-Rule-Report AVP and shall set the PCC-Rule-Status to INACTIVE.

- Time of the Day Procedures: PCEF performs PCC rule request as instructed by the PCRF. Revalidation-Time when set by the PCRF, causes the PCEF to trigger a PCRF interaction to request



PCC rules from the PCRF for an established IP CAN session. The PCEF stops the timer once the PCEF triggers a REVALIDATION\_TIMEOUT event.



**Important:** In 11.0 and later releases, Rule-Activation-Time / Rule-Deactivation-Time / Revalidation-Time AVP is successfully parsed only if its value corresponds to current time or a later time than the current IPSG time, else the AVP and entire message is rejected. In earlier releases the AVP is successfully parsed only if its value corresponds to a later time than the current IPSG time, else the AVP and entire message is rejected.

## Charging Control

Charging Control is the process of associating packets belonging to a SDF to a charging key, and applying online charging and/or offline charging, as appropriate. Flow-based charging handles differentiated charging of the bearer usage based on real time analysis of the SDFs. In order to allow for charging control, the information in the PCC rule identifies the SDF and specifies the parameters for charging control. The PCC rule information may depend on subscription data.

In the case of online charging, it is possible to apply an online charging action upon PCEF events (for example, re-authorization upon QoS change).

It is possible to indicate to the PCEF that interactions with the charging systems are not required for a PCC rule, that is to perform neither accounting nor credit control for this SDF, and then no offline charging information is generated.

Supported Features:

- Provisioning of Charging-related Information for the IP-CAN Session.
- Provisioning of Charging Addresses: Primary or secondary event charging function name (Online Charging Server (OCS) addresses or the peer names).



**Important:** In this release, provisioning of primary or secondary charging collection function name (Offline Charging Server (OFCS) addresses) over Gx is not supported.

- Provisioning of Default Charging Method: In this release, the default charging method is sent in CCR-I message. For this, new AVPs Online/Offline are sent in CCR-I message based on the configuration.

## Charging Correlation

For the purpose of charging correlation between SDF level and application level (for example, IMS) as well as on-line charging support at the application level, applicable charging identifiers and IP-CAN type identifiers are passed from the PCRF to the AF, if such identifiers are available.

For IMS bearer charging, the IP Multimedia Core Network (IM CN) subsystem and the Packet Switched (PS) domain entities are required to generate correlated charging data.

In order to achieve this, the Gateway provides the GGSN Charging Identifier (GCID) associated with the PDP context along with its address to the PCRF. The PCRF in turn sends the IMS Charging Identifier (ICID), which is provided by the P-CSCF, to the Gateway. The Gateway generates the charging records including the GCID as well as the ICID if received from PCRF, so that the correlation of charging data can be done with the billing system.

PCRF also provides the flow identifier, which uniquely identifies an IP flow in an IMS session.

## Policy and Charging Control (PCC) Rules

A PCC rule enables the detection of an SDF and provides parameters for policy control and/or charging control. The purpose of the PCC rule is to:


- Detect a packet belonging to an SDF.
  - Select downlink IP CAN bearers based on SDF filters in the PCC rule.
  - Enforce uplink IP flows are transported in the correct IP CAN bearer using the SDF filters within the PCC rule.
- Identify the service that the SDF contributes to.
- Provide applicable charging parameters for an SDF.
- Provide policy control for an SDF.

The PCEF selects a PCC rule for each packet received by evaluating received packets against SDF filters of PCC rules in the order of precedence of the PCC rules. When a packet matches a SDF filter, the packet matching process for that packet is completed, and the PCC rule for that filter is applied.

There are two types of PCC rules:

- **Dynamic PCC Rules:** Rules dynamically provisioned by the PCRF to the PCEF via the Gx interface. These PCC rules may be either predefined or dynamically generated in the PCRF. Dynamic PCC rules can be activated, modified, and deactivated at any time.
- **Predefined PCC Rule:** Rules preconfigured in the PCEF by the operators. Predefined PCC rules can be activated or deactivated by the PCRF at any time. Predefined PCC rules within the PCEF may be grouped allowing the PCRF to dynamically activate a set of PCC rules over the Gx reference point.

---


 **Important:** A third type of rule, the static PCC rule can be preconfigured in the chassis by the operators. Static PCC rules are not explicitly known in the PCRF, and are not under control of the PCRF. Static PCC rules are bound to general purpose bearer with no Gx control.

---

A PCC rule consists of:

- **Rule Name:** The rule name is used to reference a PCC rule in the communication between the PCEF and PCRF.
- **Service Identifier:** The service identifier is used to identify the service or the service component the SDF relates to.
- **Service Data Flow Filter(s):** The service flow filter(s) is used to select the traffic for which the rule applies.
- **Precedence:** For different PCC rules with overlapping SDF filter, the precedence of the rule determines which of these rules is applicable. When a dynamic PCC rule and a predefined PCC rule have the same priority, the dynamic PCC rule takes precedence.
- **Gate Status:** The gate status indicates whether the SDF, detected by the SDF filter(s), may pass (gate is open) or will be discarded (gate is closed) in uplink and/or in downlink direction.
- **QoS Parameters:** The QoS information includes the QoS class identifier (authorized QoS class for the SDF), the Allocation and Retention Priority (ARP), and authorized bitrates for uplink and downlink.

---

 **Important:** In earlier releases, ECS used only the Priority-Level part of ARP byte for bearer binding, (along with QCI). Now the entire ARP byte is used for bearer binding (along with QCI). Since the capability and vulnerability bits are optional in a dynamic rule, if a dynamic rule is received without these flags, it is assumed that the capability bit is set to 1 (disabled) and vulnerability bit is set to 0 (enabled). For predefined rules, currently configuring these two flags is

not supported, so as of now all predefined rules are assumed to have capability bit set to 1 (disabled) and vulnerability bit set to 0 (enabled).

- Charging key (rating group)
- Other charging parameters: The charging parameters define whether online and offline charging interfaces are used, what is to be metered in offline charging, on what level the PCEF will report the usage related to the rule, and so on.



**Important:** In this release, configuring the Metering Method and Reporting Level for dynamic PCC rules is not supported.

PCC rules also include Application Function (AF) record information for enabling charging correlation between the application and bearer layer if the AF has provided this information via the Rx interface. For IMS, this includes the IMS Charging Identifier (ICID) and flow identifiers.

## PCC Procedures over Gx Reference Point

### Request for PCC rules

The PCEF, via the Gx reference point, requests for PCC rules in the following instances:

- At IP-CAN session establishment.
- At IP-CAN session modification.

PCC rules can also be requested as a consequence of a failure in the PCC rule installation/activation or enforcement without requiring an event trigger.

### Provisioning of PCC rules

The PCRF indicates, via the Rel. 7 Gx reference point, the PCC rules to be applied at the PCEF. This may be using one of the following procedures:

- PULL (provisioning solicited by the PCEF): In response to a request for PCC rules being made by the PCEF, the PCRF provisions PCC rules in the CC-Answer.
- PUSH (unsolicited provisioning): The PCRF may decide to provision PCC rules without obtaining a request from the PCEF. For example, in response to information provided to the PCRF via the Rx reference point, or in response to an internal trigger within the PCRF. To provision PCC rules without a request from the PCEF, the PCRF includes these PCC rules in an RA-Request message. No CCR/CCA messages are triggered by this RA-Request.

For each request from the PCEF or upon unsolicited provision the PCRF provisions zero or more PCC rules. The PCRF may perform an operation on a single PCC rule by one of the following means:

- To activate or deactivate a PCC rule that is predefined at the PCEF, the PCRF provisions a reference to this PCC rule within a Charging-Rule-Name AVP and indicates the required action by choosing either the Charging-Rule-Install AVP or the Charging-Rule-Remove AVP.
- To install or modify a PCRF-provisioned PCC rule, the PCRF provisions a corresponding Charging-Rule-Definition AVP within a Charging-Rule-Install AVP.
- To remove a PCC rule which has previously been provisioned by the PCRF, the PCRF provisions the name of this rule as value of a Charging-Rule-Name AVP within a Charging-Rule-Remove AVP.

- If the PCRF performs the bearer binding, the PCRF may move previously installed or activated PCC rules from one IP CAN bearer to another IP CAN bearer.



**Important:** In 11.0 and later releases, the maximum valid length for a charging rule name is 63 bytes. When the length of the charging rule name is greater than 63 bytes, a charging rule report with RESOURCES\_LIMITATION as Rule-Failure-Code is sent. This charging rule report is sent only when the length of the rule name is lesser than 128 characters. When the charging rule name length is greater than or equal to 128 characters no charging rule report will be sent. In earlier releases, the length of the charging rule name constructed by PCRF was limited to 32 bytes.

## Selecting a PCC Rule for Uplink IP Packets

If PCC is enabled, the PCEF selects the applicable PCC rule for each received uplink IP packet within an IP CAN bearer by evaluating the packet against uplink SDF filters of PCRF-provided or predefined active PCC rules of this IP CAN bearer in the order of the precedence of the PCC rules.



**Important:** When a PCRF-provided PCC rule and a predefined PCC rule have the same precedence, the uplink SDF filters of the PCRF-provided PCC rule is applied first.



**Important:** In 11.0 and later releases, IMSA and ECS allow the PCRF to install two (or more) dynamic rules with the same precedence value. In earlier releases, for two distinct dynamic rules having the same precedence the second rule used to be rejected.

When a packet matches an SDF filter, the packet matching process for that packet is completed, and the PCC rule for that filter is applied. Uplink IP packets which do not match any PCC rule of the corresponding IP CAN bearer are discarded.

## Selecting a PCC Rule and IP CAN Bearer for Downlink IP Packets

If PCC is enabled, the PCEF selects a PCC rule for each received downlink IP packet within an IP CAN session by evaluating the packet against downlink SDF filters of PCRF-provided or predefined active PCC rules of all IP CAN bearers of the IP CAN session in the order of the precedence of the PCC rules.



**Important:** When a PCRF-provided PCC rule and a predefined PCC rule have the same precedence, the downlink SDF filters of the PCRF-provided PCC rule are applied first.

When a packet matches a SDF filter, the packet matching process for that packet is completed, and the PCC rule for that filter is applied. The Downlink IP Packet is transported within the IP CAN bearer where the selected PCC rule is mapped. Downlink IP packets that do not match any PCC rule of the IP CAN session are discarded.

The following procedures are also supported:

- Indication of IP-CAN Bearer Termination Implications
- Indication of IP-CAN Session Termination: When the IP-CAN session is being terminated (for example, for GPRS when the last PDP Context within the IP-CAN session is being terminated) the PCEF contacts the PCRF.
- Request of IP-CAN Bearer Termination: If the termination of the last IP CAN bearer within an IP CAN session is requested, the PCRF and PCEF apply the “Request of IP-CAN Session Termination” procedure.
- Request of IP-CAN Session Termination: If the PCRF decides to terminate an IP CAN session due to an internal trigger or trigger from the SPR, the PCRF informs the PCEF. The PCEF acknowledges to the PCRF and

instantly removes/deactivates all the PCC rules that have been previously installed or activated on that IP-CAN session.

The PCEF applies IP CAN specific procedures to terminate the IP CAN session. For GPRS, the GGSN send a PDP context deactivation request with the teardown indicator set to indicate that the termination of the entire IP-CAN session is requested. Furthermore, the PCEF applies the “Indication of IP CAN Session Termination” procedure.

In 12.0 and later releases, volume or rule information obtained from PCRF is discarded if the subscriber is going down.

## Volume Reporting Over Gx

This section describes the 3GPP Rel. 9 Volume Reporting over Gx feature, which is supported by all products supporting Rel. 7 Gx interface.

## License Requirements

The Volume Reporting over Gx is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

## Supported Standards


The Volume Reporting over Gx feature is based on the following standard:


3GPP TS 29.212 V9.3.0 (2010-06): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control over Gx reference point (Release 9).


## Feature Overview


The Volume Reporting over Gx feature provides PCRF the capability to make real-time decisions based on the data usage by subscribers.


---

 **Important:** Volume Reporting over Gx is applicable only for volume quota.

 **Important:** In release 10.0, only total data usage reporting is supported, uplink/downlink level reporting is not supported. In 10.2 and later releases, it is supported.

 **Important:** The PCEF only reports the accumulated usage since the last report for usage monitoring and not from the beginning.

 **Important:** If the usage threshold is set to zero (infinite threshold), no further threshold events will be generated by PCEF, but monitoring of usage will continue and be reported at the end of the session.

 **Important:** In 12.2 and later releases, usage reporting on bearer termination is supported.

---

The following steps explain how Volume Reporting over Gx works:

1. PCEF after receiving the message from PCRF parses the usage monitoring related AVPs, and sends the information to IMSA.
2. IMSA updates the information to ECS.
3. Once the ECS is updated with the usage monitoring information from PCRF, the PCEF (ECS) starts tracking the data usage.
4. For session-level monitoring, the ECS maintains the amount of data usage.
5. For PCC rule monitoring, usage is monitored with the monitoring key as the unique identifier. Each node maintains the usage information per monitoring key. When the data traffic is passed, the usage is checked against the usage threshold values and reported as described in the *Usage Reporting* section.
6. The PCEF continues to track data usage after the threshold is reached and before a new threshold is provided by the PCRF. If a new usage threshold is not provided by the PCRF in the acknowledgement of an IP-CAN Session modification where its usage was reported, then usage monitoring does not continue in the PCEF for that IP CAN session.

## Usage Monitoring

- **Usage Monitoring at Session Level:** PCRF subscribes to the session-level volume reporting over Gx by sending the Usage-Monitoring-Information AVP with the usage threshold level set in Granted-Service-Unit AVP and Usage-Monitoring-Level AVP set to SESSION\_LEVEL(0). After the AVPs are parsed by DPCA, IMSA updates the information to ECS. Once ECS is updated usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present. In 11.0 and later releases, Monitoring Key at session level is supported.

In 12.0 and later releases, enabling and disabling session usage in a single message from PCRF is supported. This is supported only if the monitoring key is associated at session level.

In 12.0 and later releases, monitoring of usage based on input/output octet threshold levels is supported. Usage is reported based on the enabled threshold level. If multiple levels are enabled, usage will be reported on all the enabled levels even if only one of the levels is breached. Monitoring will be stopped on the missing threshold levels in the response for the usage report from PCRF (expected to provide the complete set again if PCRF wants to continue monitoring on the multiple levels enabled earlier).

Total threshold level along with UL/DL threshold level in the GSU AVP is treated as an error and only total threshold level is accepted.

- **Usage Monitoring at Flow Level:** PCRF subscribes to the flow-level volume reporting over Gx by sending the Usage-Monitoring-Information AVP with the usage threshold level set in Granted-Service-Unit AVP and Usage-Monitoring-Level AVP set to PCC\_RULE\_LEVEL(1). Monitoring Key is mandatory in case of a flow-level monitoring since the rules are associated with the monitoring key and enabling/disabling of usage monitoring at flow level can be controlled by PCRF using it. After the AVPs are parsed by DPCA, IMSA updates the information to ECS. Once ECS is updated usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present.

Usage monitoring is supported for static, predefined rules, and dynamic rule definitions.

- **Usage Monitoring for Static Rules:** In the case of static rules, the usage reporting on last rule removal associated with the monitoring key is not applicable. In this case only the usage monitoring information is received from the PCRF.
- **Usage Monitoring for Predefined Rules:** If the usage monitoring needs to be enabled for the predefined rules, PCRF sends the rule and the usage monitoring information containing the monitoring key and the usage threshold. The Monitoring key should be same as the one pre-configured in PCEF for that predefined rule. There can be multiple rules associated with the same monitoring key. Hence enabling a particular monitoring key would result in the data being tracked for multiple rules having the same

monitoring key. After DPCA parses the AVPs IMSA updates the information to ECS. Once ECS is updated usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present.

- **Usage Monitoring for Dynamic Rules:** If the usage monitoring needs to be enabled for dynamic ruledefs, PCRF provides the monitoring key along with a charging rule definition and the usage monitoring information containing the monitoring key and the usage threshold. This would result in the usage monitoring being done for all the rules associated with that monitoring key. After DPCA parses the AVPs, IMSA updates the information to ECS. Once ECS is updated, the usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present. Monitoring key for dynamic ruledef is dynamically assigned by PCRF which is the only difference with predefined rules in case of usage monitoring.

## Usage Reporting

Usage at subscriber/flow level is reported to PCRF under the following conditions:

- **Usage Threshold Reached:** PCEF records the subscriber data usage and checks if the usage threshold provided by PCRF is reached. This is done for both session and rule level reporting.

For session-level reporting, the actual usage volume is compared with the usage volume threshold.

For rule-level reporting the rule that hits the data traffic is used to find out if the monitoring key is associated with it, and based on the monitoring key the data usage is checked. Once the condition is met, it reports the usage information to IMSA and continues monitoring. IMSA then triggers the CCR-U if “USAGE\_REPORT” trigger is enabled by the PCRF. The Usage-Monitoring-Information AVP is sent in this CCR with the “Used-Service-Unit” set to the amount of data usage by subscriber.

If PCRF does not provide a new usage threshold in the usage monitoring information as a result of CCR from PCEF when the usage threshold is reached, the usage monitoring is stopped at PCEF and no usage status is reported.

In the non-standard Volume Reporting over Gx implementation, usage monitoring will be stopped once the threshold is breached, else the monitoring will continue. There will be no further usage reporting until the CCA is received.

- **Usage Monitoring Disabled:** If the PCRF explicitly disables the usage monitoring with Usage-Monitoring-Support AVP set to USAGE\_MONITORING\_DISABLED, the PCEF stops monitoring and reports the usage information (when the monitoring was enabled) to PCRF if the usage monitoring is disabled by PCRF as a result of CCR from PCEF which is not related to reporting usage, other external triggers, or a PCRF internal trigger. If the PCRF does not provide a new usage threshold as a result of CCR from PCEF when the usage threshold is reached, the usage monitoring is stopped at PCEF and no further usage status is reported.
- **IP CAN Session Termination:** When the IP CAN session is terminated, the accumulated subscriber usage information is reported to PCRF in the CCR-T from PCEF. If PCC usage level information is enabled by PCRF, the PCC usage will also be reported.
- **PCC Rule Removal:** When the PCRF deactivates the last PCC rule associated with a usage monitoring key, the PCEF sends a CCR with the data usage for that monitoring key. If the PCEF reports the last PCC rule associated with a usage monitoring key is inactive, the PCEF reports the accumulated usage for that monitoring key within the same CCR command if the Charging-Rule-Report AVP was included in a CCR command; otherwise, if the Charging-Rule-Report AVP was included in an RAA command, the PCEF sends a new CCR command to report accumulated usage for the usage monitoring key. In 12.0 and later releases, usage reporting on last rule deactivation using rule deactivation time set by PCRF is supported.
- **PCRF Requested Usage Report:** In 10.2 and later releases, the accumulated usage since the last report is sent even in case of immediate reporting, the usage is reset after immediate reporting and usage monitoring

continued so that the subsequent usage report will have the usage since the current report. In earlier releases the behavior was to accumulate the so far usage in the next report.

- Release 12.2 onwards, usage reporting on bearer termination can be added. When a bearer is deleted due to some reason, the rules associated with the bearer will also be removed. So, the usage will be reported on the monitoring key(s) whose associated rule is the last one that is removed because of bearer termination.
- Revalidation Timeout: In the non-standard implementation, if usage monitoring and reporting is enabled and a revalidation timeout occurs, the PCEF sends a CCR to request PCC rules and reports all accumulated usage for all enabled monitoring keys since the last report (or since usage reporting was enabled if the usage was not yet reported) with the accumulated usage at IP-CAN session level (if enabled) and at service data flow level (if enabled) This is the default behavior.

In the case of standard implementation, this must be enabled by CLI configuration.



**Important:** The Usage Reporting on Revalidation Timeout feature is available by default in non-standard implementation of Volume Reporting over Gx. In 10.2 and later releases, this is configurable in the standard implementation. This is not supported in 10.0 release for standard based volume reporting.

Once the usage is reported, the usage counter is reset to zero. The PCEF continues to track data usage from the zero value after the threshold is reached and before a new threshold is provided by the PCRF. If a new usage threshold is not provided by the PCRF in the acknowledgement of an IP-CAN Session modification where its usage was reported, then usage monitoring does not continue in the PCEF for that IP CAN session and the usage accumulated between the CCR-CCA will be discarded.

For information on how to configure the Volume Reporting over Gx feature, see the [Configuring Volume Reporting over Gx](#) section.

## How Rel. 7 Gx Works

This section describes how dynamic policy and charging control for subscribers works with Rel. 7 Gx interface support in GPRS/UMTS networks.

The following figure and table explain the IMSA process between a system and IMS components that is initiated by the UE.

In this example, the Diameter Policy Control Application (DPCA) is the Gx interface to the PCRF. The interface between IMSA with PCRF is the Gx interface, and the interface between Session Manager (SessMgr) and Online Charging Service (OCS) is the Gy interface. Note that the IMSA service and DPCA are part of SessMgr on the system and separated in the figure for illustration purpose only.



Figure 41. Rel. 7 Gx IMS Authorization Call Flow

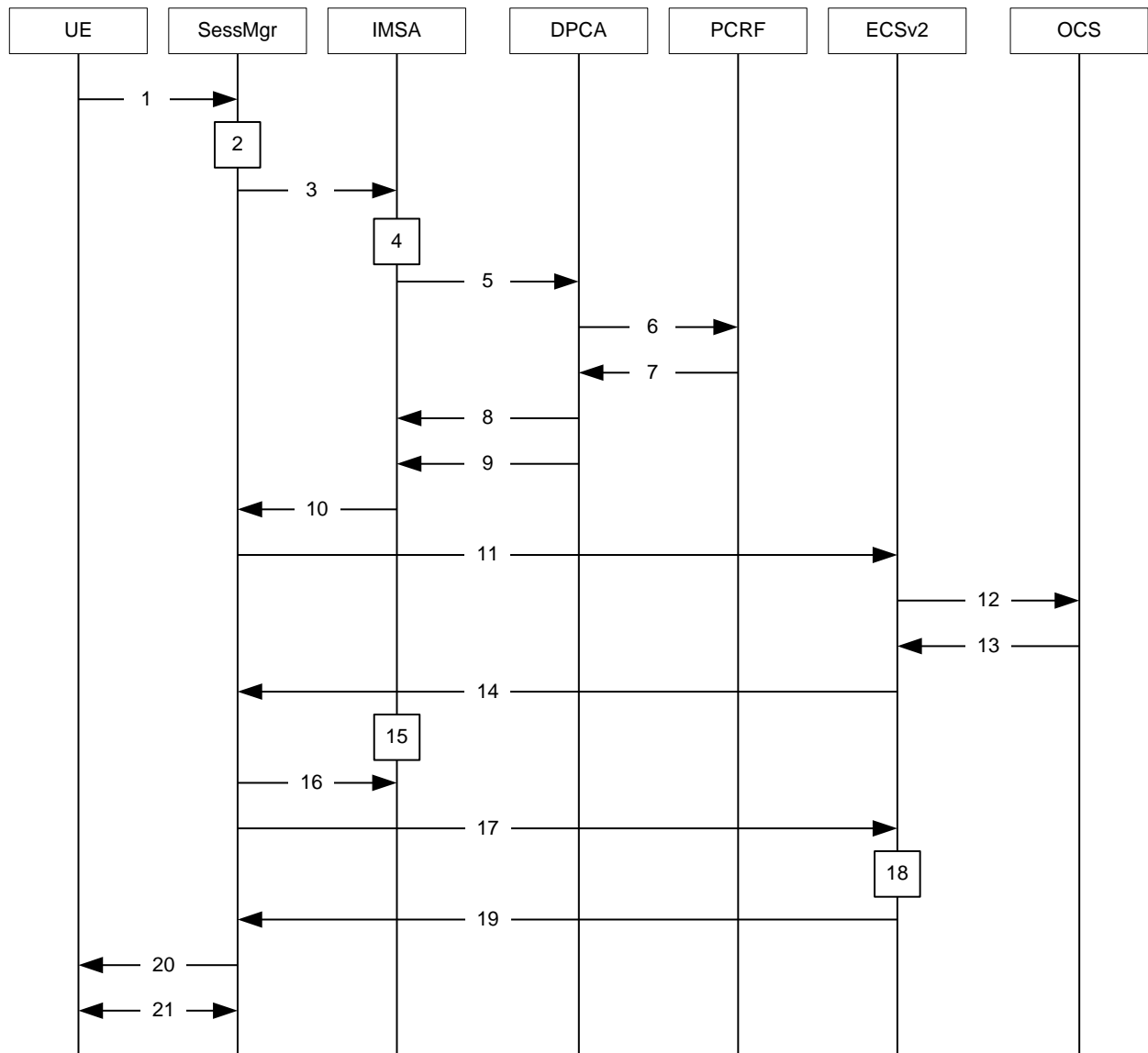


Table 17. Rel. 7 Gx IMS Authorization Call flow Description

Step	Description
1	UE (IMS subscriber) requests for primary PDP context activation/creation.
2	SessMgr allocates an IP address to the UE.
3	SessMgr requests IMS Authorization, if IMSA is enabled for the APN.
4	IMSA allocates resources for the IP CAN session and the bearer, and selects the PCRF to contact based on the user's selection key (for example, msisdn).
5	IMSA requests the DPCA module to issue an auth request to the PCRF.

Step	Description
6	DPCA sends a CCR initial message to the selected PCRF. This message includes the Context-Type AVP set to PRIMARY and the IP address allocated to the UE. The message may include the Bearer-Usage AVP set to GENERAL. The Bearer-Operation is set to Establishment. The Bearer ID is included if the PCRF does the bearer binding.
7	PCRF may send preconfigured charging rules in CCA, if a preconfigured rule set for general purpose PDP context is provided in PCRF. The dynamic rules and the authorized QoS parameters could also be included by the PCRF.
8	DPCA passes the charging rule definition, charging rule install, QoS information received from the PCRF, event triggers, and so on, along with the Bearer ID that corresponds to the rules received from the PCRF to IMSA. IMSA stores the information. If the Bearer ID is absent, and PCRF does the bearer binding, the rule is skipped. Whereas, if the Bearer ID is absent and the PCEF does the bearer binding, the rule is passed onto the ECS to perform bearer binding.
9	DPCA calls the callback function registered with it by IMSA.
10	IMSA stores the bearer authorized QoS information and notifies the SessMgr. Other PCRF provided information common to the entire PDP session (event trigger, primary/secondary OCS address, and so on) is stored within the IMSA. After processing the information, IMSA notifies the SessMgr about the policy authorization complete.
11	If the validation of the rules fails in IMSA/DPCA, a failure is notified to PCRF containing the Charging-Rule-Report AVP. Else, IMSA initiates creation of ECS session. The APN name, primary/secondary OCS server address, and so on are sent to the ECS from the SessMgr.
12	ECS performs credit authorization by sending CCR(I) to OCS with CC-Request-Type set to INITIAL_REQUEST to open the credit control session. This request includes the active Rulebase-Id (default rulebase ID from the APN/AAA) and GPRS specific attributes (for example, APN, UMTS QoS, and so on).
13	OCS returns a CCA initial message that may activate a statically configured Rulebase and may include preemptive quotas.
14	ECS responds to SessMgr with the response message.
15	SessMgr requests IMSA for the dynamic rules.
16	IMSA sends the dynamic rules to SessMgr. Note that until the primary PDP context is established, all RAR messages from the PCRF are rejected.
17	SessMgr sends the dynamic rule information to the ECS. The gate flow status information and the QoS per flow (charging rule) information are also sent in the message.
18	ECS activates the predefined rules received, and installs the dynamic rules received. Also, the gate flow status and the QoS parameters are updated by ECS as per the dynamic charging rules. The Gx rulebase is treated as an ECS group-of-ruledefs. The response message contains the Charging Rule Report conveying the status of the rule provisioning at the ECS. ECS performs PCEF bearer binding for rules without bearer ID.
19	If the provisioning of rules fails partially, the context setup is accepted, and a new CCR-U is sent to the PCRF with the Charging-Rule-Report containing the PCC rule status for the failed rules. If the provisioning of rules fails completely, the context setup is rejected.
20	Depending on the response for the PDP Context Authorization, SessMgr sends the response to the UE and activates/rejects the call. If the Charging-Rule-Report contains partial failure for any of the rules, the PCRF is notified, and the call is activated. If the Charging-Rule-Report contains complete failure, the call is rejected.
21	Based on the PCEF bearer binding for the PCC rules at Step 18, the outcome could be one or more network-initiated PDP context procedures with the UE (Network Requested Update PDP Context (NRUPC) / Network Requested Secondary PDP Context Activation (NRSPCA)).

## Configuring Rel. 7 Gx Interface

To configure Rel. 7 Gx interface functionality, the IMS Authorization service must be configured at the context level, and then the APN configured to use the IMS Authorization service.

To configure Rel. 7 Gx interface functionality:

- Step 1** Configure IMS Authorization service at the context level for IMS subscriber in GPRS/UMTS network as described in the [Configuring IMS Authorization Service at Context Level](#) section.
- Step 2** Verify your configuration as described in the [Verifying the Configuration](#) section.
- Step 3** Configure an APN within the same context to use the IMS Authorization service for IMS subscriber as described in the [Applying IMS Authorization Service to an APN](#) section.
- Step 4** Verify your configuration as described in the [Verifying Subscriber Configuration](#) section.
- Step 5** *Optional:* Configure the Volume Reporting over Gx feature as described in the [Configuring Volume Reporting over Gx](#) section.
- Step 6** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.



**Important:** Commands used in the configuration examples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the *Command Line Interface Reference* for complete information regarding all commands.

## Configuring IMS Authorization Service at Context Level

Use the following example to configure IMS Authorization service at context level for IMS subscribers in GPRS/UMTS networks:

```
configure

context <context_name>

    ims-auth-service <imsa_service_name>

        p-cscf discovery table { 1 | 2 } algorithm { ip-address-modulus | msisdn-modulus
| round-robin }

        p-cscf table { 1 | 2 } row-precedence <precedence_value> { address <ip_address>
| ipv6-address <ipv6_address> } [ secondary { address <ip_address> | ipv6-address
<ipv6_address> } ]

    policy-control

        diameter origin endpoint <endpoint_name>

        diameter dictionary <dictionary>
```

```

diameter request-timeout <timeout_duration>

diameter host-select table { { { 1 | 2 } algorithm { ip-address-modulus |
msisdn-modulus | round-robin } } | prefix-table { 1 | 2 } }

diameter host-select row-precedence <precedence_value> table { { { 1 | 2 }
host <host_name> [ realm <realm_id> ] [ secondary host <host_name> [ realm <realm_id> ] ]
} | { prefix-table { 1 | 2 } msisdn-prefix-from <msisdn_prefix_from> msisdn-prefix-to
<msisdn_prefix_to> host <host_name> [ realm <realm_id> ] [ secondary host <sec_host_name>
[ realm <sec_realm_id> ] algorithm { active-standby | round-robin } ] } } [ -noconfirm ]

diameter host-select reselect subscriber-limit <subscriber_limit> time-
interval <duration>

failure-handling cc-request-type { any-request | initial-request | terminate-
request | update-request } { diameter-result-code { any-error | <result_code> [ to
<end_result_code> ] } } { continue | retry-and-terminate | terminate }

end

```

## Notes:

- <context\_name> must be the name of the context where you want to enable IMS Authorization service.
- <imsa\_service\_name> must be the name of the IMS Authorization service to be configured for Rel. 7 Gx interface authentication.
- A maximum of 16 authorization services can be configured globally in a system. There is also a system limit for the maximum number of total configured services.
- To enable Rel. 7 Gx interface support, pertinent Diameter dictionary must be configured. For information on the specific Diameter dictionary to use, please contact your local service representative.
- When configuring the MSISDN prefix range based PCRF selection mechanism:

To enable the Gx interface to connect to a specific PCRF for a range of subscribers configure **msisdn-prefix-from** <msisdn\_prefix\_from> and **msisdn-prefix-to** <msisdn\_prefix\_to> with the starting and ending MSISDNs respectively.

To enable the Gx interface to connect to a specific PCRF for a specific subscriber, configure both **msisdn-prefix-from** <msisdn\_prefix\_from> and **msisdn-prefix-to** <msisdn\_prefix\_to> with the same MSISDN.

In StarOS 8.1 and later releases, per MSISDN prefix range table a maximum of 128 rows can be added. In StarOS 8.0 and earlier releases, a maximum of 100 rows can be added.

The MSISDN ranges must not overlap between rows.

- The Round Robin algorithm for PCRF selection is effective only over a large number of PCRF selections, and not at a granular level.
- *Optional:* To configure the Quality of Service (QoS) update timeout for a subscriber, in the IMS Authorization Service Configuration Mode, enter the following command:

```
qos-update-timeout <timeout_duration>
```

- *Optional:* To configure signalling restrictions, in the IMS Authorization Service Configuration Mode, enter the following commands:

```
signaling-flag { deny | permit }
```

```
signaling-flow permit server-address <ip_address> [ server-port { <port_number> |
range <start_number> to <end_number> } ] [ description <string> ]
```

- *Optional:* To configure action on packets that do not match any policy gates in the general purpose PDP context, in the IMS Authorization Service Configuration Mode, enter the following command:

```
traffic-policy general-pdp-context no-matching-gates direction { downlink | uplink
} { forward | discard }
```

- To configure the PCRF host destinations configured in the GGSN/PCEF, use the **diameter host-select** CLI commands.
- To configure the GGSN/PCEF to use a pre-defined rule when the Gx fails, set the **failure-handling cc-request-type** CLI to **continue**. Policies available/in use will continue to be used and there will be no further interaction with the PCRF.
- For provisioning of default charging method, use the following configurations. For this, the AVPs Online and Offline will be sent in CCR-I message based on the configuration.

- To send Enable Online:

```
configure
active-charging service <ecs_service_name>
charging-action <charging_action_name>
cca charging credit
exit
```

- To send Enable Offline:

```
configure
active-charging service <ecs_service_name>
rulebase <rulebase_name>
billing-records rf
exit
```

## Verifying the Configuration

To verify the IMS Authorization service configuration:

- Step 1** Change to the context where you enabled IMS Authorization service by entering the following command:

```
context <context_name>
```

- Step 2** Verify the IMS Authorization service's configurations by entering the following command:

```
show ims-authorization service name <imsa_service_name>
```

## Applying IMS Authorization Service to an APN

After configuring IMS Authorization service at the context-level, an APN within the same context must be configured to use the IMS Authorization service for an IMS subscriber.

Use the following example to apply IMS Authorization service functionality to a previously configured APN within the context configured in the [Configuring Rel. 7 Gx Interface](#) section.

**configure**

```

context <context_name>

    apn <apn_name>

        ims-auth-service <imsa_service_name>

        active-charging rulebase <rulebase_name>

    end

```

## Notes:

- <context\_name> must be the name of the context in which the IMS Authorization service was configured.
- <imsa\_service\_name> must be the name of the IMS Authorization service configured for IMS authentication in the context.
- For Rel. 7 Gx, the ECS rulebase must be configured in the APN.
- ECS allows change of rulebase via Gx for PCEF binding scenarios. When the old rulebase goes away, all the rules that were installed from that rulebase are removed. This may lead to termination of a few bearers (PDP contexts) if they are left without any rules. If there is a Gx message that changes the rulebase, and also activates some predefined rules, the rulebase change is made first, and the rules are activated from the new rulebase. Also, the rulebase applies to the entire call. All PDP contexts (bearers) in one call use the same ECS rulebase.
- For predefined rules configured in the ECS, MBR/GBR of a dynamic/predefined rule is checked before it is used for PCEF binding. All rules (dynamic as well as predefined) have to have an MBR associated with them and all rules with GBR QCI should have GBR also configured. So for predefined rules, one needs to configure appropriate peak-data-rate, committed-data-rate as per the QCI being GBR QCI or non-GBR QCI. For more information, in the ACS Charging Action Configuration Mode, see the **flow limit-for-bandwidth** CLI command.
- Provided interpretation of the Gx rulebase is chosen to be ECS group-of-ruledefs, in the Active Charging Service Configuration Mode configure the following command:

```
policy-control charging-rule-base-name active-charging-group-of-ruledefs
```

## Verifying Subscriber Configuration

Verify the IMS Authorization service configuration for subscriber(s) by entering the following command:

```
show subscribers ims-auth-service <imsa_service_name>
```

<imsa\_service\_name> must be the name of the IMS Authorization service configured for IMS authentication.

## Configuring Volume Reporting over Gx

This section describes the configuration required to enable Volume Reporting over Gx.

To enable Volume Reporting over Gx, use the following configuration:

**configure**

```

active-charging service <ecs_service_name>

    rulebase <rulebase_name>

```

```

    action priority <priority> dynamic-only ruledef <ruledef_name> charging-action
    <charging_action_name> monitoring-key <monitoring_key>

    exit

exit

context <context_name>

    ims-auth-service <imsa_service_name>

    policy-control

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

    end

```

## Notes:

- The maximum accepted monitoring key value by the PCEF is 4294967295. If the PCEF sends a greater value, the value is converted to an Unsigned Integer value.
- The **event-update** CLI which enables volume usage report to be sent in event updates is available only in 10.2 and later releases. The optional keyword **reset-usage** enables to support delta reporting wherein the usage is reported and reset at PCEF. If this option is not configured, the behavior is to send the usage information as part of event update but not reset at PCEF.

## Gathering Statistics

This section explains how to gather Rel. 7 Gx statistics and configuration information.

In the following table, the first column lists what statistics to gather, and the second column lists the action to perform.

**Table 18. Gathering Rel. 7 Gx Statistics and Information**

Statistics/Information	Action to perform
Information and statistics specific to policy control in IMS Authorization service.	<b>show ims-authorization policy-control statistics</b>
Information and statistics specific to the authorization servers used for IMS Authorization service.	<b>show ims-authorization servers ims-auth-service</b>
Information of all IMS Authorization service.	<b>show ims-authorization service all</b>
Statistics of IMS Authorization service.	<b>show ims-authorization service statistics</b>
Information, configuration, and statistics of sessions active in IMS Authorization service.	<b>show ims-authorization sessions all</b>
Complete information, configuration, and statistics of sessions active in IMS Authorization service.	<b>show ims-authorization sessions full</b>
Summarized information of sessions active in IMS Authorization service.	<b>show ims-authorization sessions summary</b>

Statistics/Information	Action to perform
Complete statistics for active charging service sessions.	<code>show active-charging sessions full</code>
Information for all rule definitions configured in the service.	<code>show active-charging ruledef all</code>
Information for all rulebases configured in the system.	<code>show active-charging rulebase all</code>
Information on all group of ruledefs configured in the system.	<code>show active-charging group-of-ruledefs all</code>
Information on policy gate counters and status.	<code>show ims-authorization policy-gate { counters   status }</code>



## Rel. 8 Gx Interface

Rel. 8 Gx interface support is available on the Cisco ASR chassis running StarOS 10.0 or StarOS 11.0 and later releases.

This section describes the following topics:

- [HA/PDSN Rel. 8 Gx Interface Support](#)
- [P-GW Rel. 8 Gx Interface Support](#)

## HA/PDSN Rel. 8 Gx Interface Support

This section provides information on configuring Rel. 8 Gx interface for HA and PDSN to support policy and charging control for subscribers in CDMA networks.

The IMS service provides application support for transport of voice, video, and data independent of access support. Roaming IMS subscribers in CDMA networks require apart from other functionality sufficient, uninterrupted, consistent, and seamless user experience during an application session. It is also important that a subscriber gets charged only for the resources consumed by the particular IMS application used.

It is recommended that before using the procedures in this section you select the configuration example that best meets your service model, and configure the required elements for that model as described in this Administration Guide.

This section describes the following topics:

- [Introduction](#)
- [Terminology and Definitions](#)
- [How it Works](#)
- [Configuring HA/PDSN Rel. 8 Gx Interface Support](#)
- [Gathering Statistics](#)

## Introduction

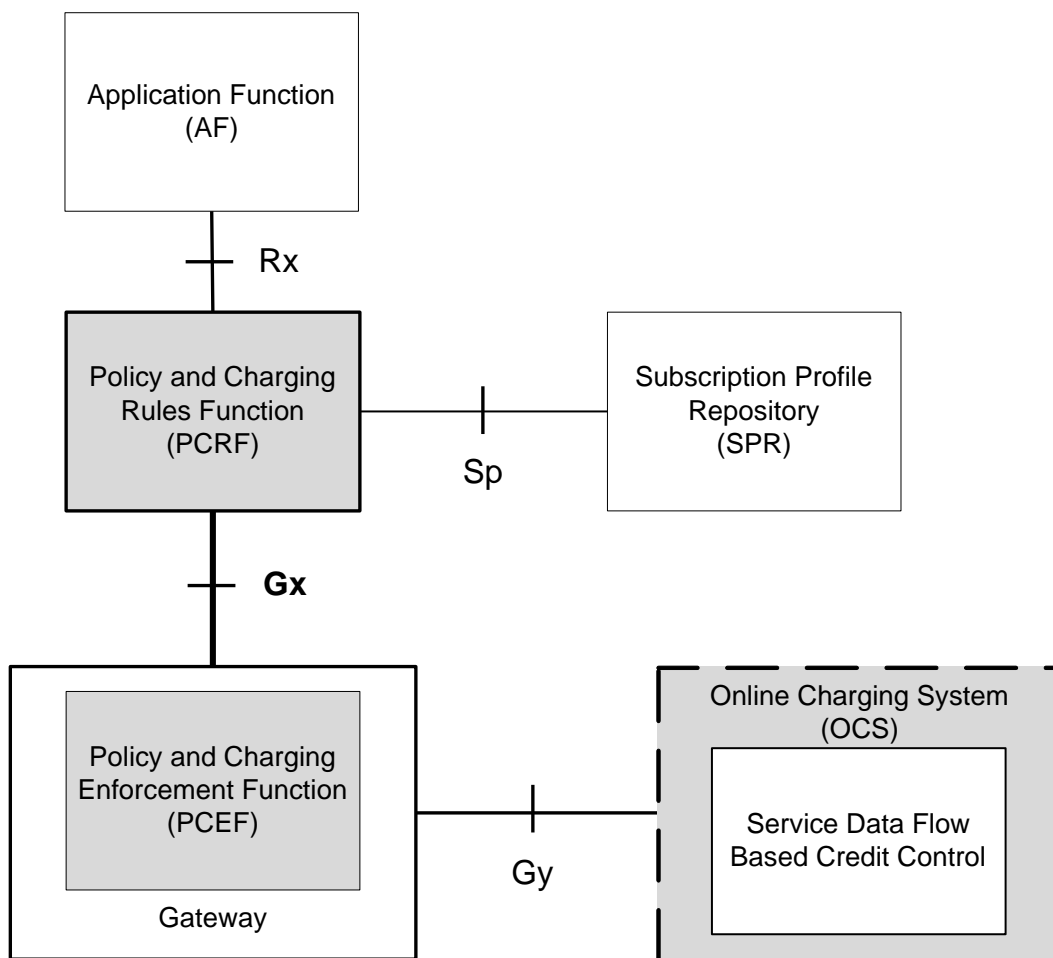
For IMS deployment in CDMA networks the system uses Rel. 8 Gx interface for policy-based admission control support and flow-based charging (FBC). The Rel. 8 Gx interface supports enforcing policy control features like gating, bandwidth limiting, and so on, and also supports FBC. This is accomplished via dynamically provisioned Policy Control and Charging (PCC) rules. These PCC rules are used to identify Service Data Flows (SDF) and to 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 FBC control. In the PCC architecture, this is accomplished mainly by the Policy and Charging Enforcement Function (PCEF)/HA/PDSN and the Policy and Charging Rules Function (PCRF). The client functionality lies with the HA/PDSN, therefore in the IMS Authorization (IMSA) scenario it is also called the Gateway. The PCEF function is provided by the Enhanced Charging Service (ECS). The Gx interface is implemented as a Diameter connection. The Gx messaging mostly involves installing/modifying/removing dynamic rules and activating/deactivating predefined rules.

The Gx reference point is located between the Gateway/PCEF and the PCRF. This reference point is used for provisioning and removal of PCC rules from the PCRF to the Gateway/PCEF, and the transmission of traffic plane events from the Gateway/PCEF to the PCRF. The Gx reference point can be used for charging control, policy control, or both by applying AVPs relevant to the application.

The following figure shows the reference points between elements involved in the policy and charging architecture.

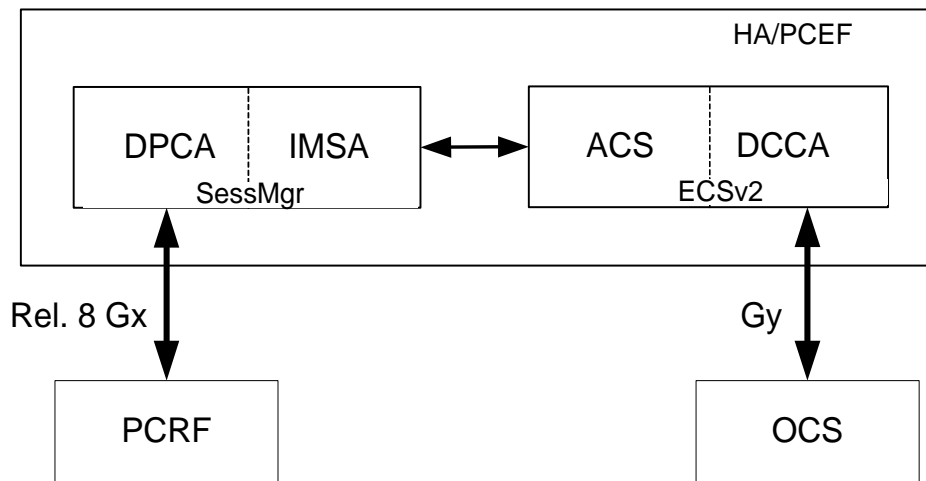
Figure 42. HA/PDSN Rel. 8 Gx PCC Logical Architecture



Within the Gateway, the IMSA and DPCA modules handle the Gx protocol related functions (at the SessMgr) and the policy enforcement and charging happens at ECS. The Gy protocol related functions are handled within the DCCA module (at the ECS).

The following figure shows the interaction between components within the Gateway.

Figure 43. HA/PDSN Rel. 8 Gx PCC Architecture within PCEF



## License Requirements

The HA/PDSN Rel. 8 Gx interface support is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

## Supported Standards

HA/PDSN Rel. 8. Gx interface support is based on the following standards and RFCs:

- 3GPP TS 23.203 V8.3.0 (2008-09) 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Policy and charging control architecture (Release 8)
- 3GPP TS 29.212 V8.6.0 (2009-12) 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control over Gx reference point (Release 8)
- 3GPP TS 29.213 V8.1.1 (2008-10) 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control signalling flows and QoS parameter mapping; (Release 8)
- RFC 3588, Diameter Base Protocol; September 2003
- RFC 4006, Diameter Credit-Control Application; August 2005

## Terminology and Definitions

This section describes features and terminology pertaining to HA/PDSN Rel. 8 Gx functionality.

## Policy Control

The process whereby the PCRF indicates to the PCEF how to control the IP-CAN session.

Policy control comprises the following functions:

- Binding
- Gating Control

- Event Reporting
- QoS Control
- Other Features

## Binding

In the HA/PDSN Rel. 8 Gx implementation, since there are no bearers within a MIP session the IP-CAN Bearer concept does not apply. Only authorized IP-CAN session is applicable.


## Gating Control

Gating control is the blocking or allowing of packets belonging to an SDF, to pass through to the desired endpoint. A gate is described within a PCC rule and gating control is applied on a per SDF basis. The commands to open or close the gate leads to the enabling or disabling of the passage for corresponding IP packets. If the gate is closed, all packets of the related IP flows are dropped. If the gate is open, the packets of the related IP flows are allowed to be forwarded.

## Event Reporting

---

 **Important:** Unconditional reporting of event triggers from PCRF to PCEF when PCEF has not requested for is not supported.

 **Important:** In the HA/PDSN Rel. 8 Gx implementation, only the AN\_GW\_CHANGE (21) event trigger is supported.


---

Event reporting is the notification of and reaction to application events to trigger new behavior in the user plane as well as the reporting of events related to the resources in the Gateway (PCEF). Event triggers may be used to determine which IP-CAN session modification or specific event causes the PCEF to re-request PCC rules. Event trigger reporting from PCEF to PCRF, and provisioning of event triggers happens at IP-CAN session level.

The Event Reporting Function (ERF) located in the PCEF, receives event triggers from PCRF during the Provision of PCC Rules procedure and performs event trigger detection. When an event matching the received event trigger occurs, the ERF reports the occurred event to the PCRF. If the provided event triggers are associated with certain parameter values then the ERF includes those values in the response to the PCRF.

## QoS Control

---

 **Important:** In the HA/PDSN Rel. 8 Gx implementation, only authorized IP-CAN Session is supported. Provisioning of authorized QoS per IP-CAN bearer, policy enforcement for authorized QoS per QCI, and coordination of authorized QoS scopes in mixed mode are not applicable.

---

QoS control is the authorization and enforcement of the maximum QoS that is authorized for an SDF. In case of an aggregation of multiple SDFs, the combination of the authorized QoS information of the individual SDFs is provided as the authorized QoS for this aggregate. QoS control per SDF allows the PCC architecture to provide the PCEF with the authorized QoS to be enforced for each specific SDF.

QoS authorization information may be dynamically provisioned by the PCRF, or it can be a predefined PCC rule in the PCEF. For a predefined PCC rule within the PCEF, the authorized QoS information takes affect when the PCC rule is activated. The PCEF combines the different sets of authorized QoS information, that is the information received from the PCRF and the information corresponding to the predefined PCC rules. The PCRF knows the authorized QoS

information of the predefined PCC rules and takes this information into account when activating them. This ensures that the combined authorized QoS of a set of PCC rules that are activated by the PCRF is within the limitations given by the subscription and operator policies regardless of whether these PCC rules are dynamically provided, predefined, or both.

Supported features include:

- Provisioning and Policy Enforcement of Authorized QoS: The PCRF may provide authorized QoS to the PCEF. The authorized QoS provides appropriate values for resources to be enforced.
- Policy Provisioning for Authorized QoS Per SDF: The provisioning of authorized QoS per SDF is a part of PCC rule provisioning procedure.
- Policy Enforcement for Authorized QoS Per SDF: If an authorized QoS is defined for a PCC rule, the PCEF limits the data rate of the SDF corresponding to that PCC rule not to exceed the maximum authorized bandwidth for the PCC rule by discarding packets exceeding the limit.
- Upon deactivation or removal of a PCC rule, the PCEF frees the resources reserved for that PCC rule.

## Other Features

This section describes some of the other features.

## PCC Rule Error Handling

If the installation/activation of one or more PCC rules fails, the PCEF communicates the failure to the PCRF by including one or more Charging-Rule-Report AVP(s) in either a CCR or an RAA command for the affected PCC rules. Within each Charging-Rule-Report AVP, the PCEF identifies the failed PCC rule(s) by including the Charging-Rule-Name AVP(s) or Charging-Rule-Base-Name AVP(s), identifies the failed reason code by including a Rule-Failure-Code AVP, and includes the PCC-Rule-Status AVP.

If the installation/activation of one or more new PCC rules (that is, rules that were not previously successfully installed) fail, the PCEF sets the PCC-Rule-Status to INACTIVE for both the PUSH and the PULL modes.

If a PCC rule was successfully installed/activated, but can no longer be enforced by the PCEF, the PCEF sends the PCRF a new CCR command and includes the Charging-Rule-Report AVP. The PCEF includes the Rule-Failure-Code AVP within the Charging-Rule-Report AVP and sets the PCC-Rule-Status to INACTIVE.

In the HA/PDSN Gx implementation, the following rule failure codes are supported:

- RATING\_GROUP\_ERROR (2)
- SERVICE\_IDENTIFIER\_ERROR (3)
- GW/PCEF\_MALFUNCTION (4)
- RESOURCES\_LIMITATION (5)

If the installation/activation of one or more PCC rules fails during RAR procedure, the RAA command is sent with the Experimental-Result-Code AVP set to DIAMETER\_PCC\_RULE\_EVENT (5142).

## Time of the Day Procedures

PCEF performs PCC rule request as instructed by the PCRF. Revalidation-Time when set by the PCRF, causes the PCEF to trigger a PCRF interaction to request PCC rules from the PCRF for an established IP-CAN session. The PCEF stops the timer once the PCEF triggers a REVALIDATION\_TIMEOUT event.

When installed, the PCC rule is inactive. If Rule-Activation-Time / Rule-Deactivation-Time is specified, then the PCEF sets the rule active / inactive after that time.

## Charging Control



**Important:** In the HA/PDSN Rel. 8 Gx implementation, offline charging is not supported.

Charging Control is the process of associating packets belonging to an SDF to a charging key, and applying online charging as appropriate. FBC handles differentiated charging of the bearer usage based on real-time analysis of the SDFs. In order to allow for charging control, the information in the PCC rule identifies the SDF and specifies the parameters for charging control. The PCC rule information may depend on subscription data.

Online charging is supported via the Gy interface. In the case of online charging, it is possible to apply an online charging action upon PCEF events (for example, re-authorization upon QoS change).

It is possible to indicate to the PCEF that interactions with the charging systems are not required for a PCC rule, that is to perform neither accounting nor credit control for this SDF, then neither online nor offline charging is performed.

Supported Features:

- Provisioning of charging-related information for the IP-CAN Session
- Provisioning of charging addresses: Primary or secondary event charging function name (Online Charging Server (OCS) addresses)



**Important:** In the HA/PDSN Rel. 8 Gx implementation, provisioning of primary or secondary charging collection function name (Offline Charging Server (OFCS) addresses) over Gx is not supported.

- Provisioning of Default Charging Method

## Charging Correlation

In the HA/PDSN Rel. 8 Gx implementation, Charging Correlation is not supported. PCRF provides the flow identifier, which uniquely identifies an IP flow in an IMS session.

## Policy and Charging Control (PCC) Rules

A PCC rule enables the detection of an SDF and provides parameters for policy control and/or charging control. The purpose of the PCC rule is to:

- Detect a packet belonging to an SDF in case of both uplink and downlink IP flows based on SDF filters in the PCC rule (packet rule matching).

If no PCC rule matches the packet, the packet is dropped.

- Identify the service that the SDF contributes to.
- Provide applicable charging parameters for an SDF.
- Provide policy control for an SDF.

The PCEF selects a PCC rule for each packet received by evaluating received packets against SDF filters of PCC rules in the order of precedence of the PCC rules. When a packet matches an SDF filter, the packet matching process for that packet is completed, and the PCC rule for that filter is applied.

There are two types of PCC rules:

- **Dynamic PCC Rules:** Rules dynamically provisioned by the PCRF to the PCEF via the Gx interface. These PCC rules may be either predefined or dynamically generated in the PCRF. Dynamic PCC rules can be activated, modified, and deactivated at any time.

- **Predefined PCC Rule:** Rules preconfigured in the PCEF by the operators. Predefined PCC rules can be activated or deactivated by the PCRF at any time. Predefined PCC rules within the PCEF may be grouped allowing the PCRF to dynamically activate a set of PCC rules over the Gx reference point.



**Important:** A third kind of rule, the static PCC rule can be preconfigured in the chassis by the operators. Static PCC rules are not explicitly known in the PCRF, and are not under control of the PCRF. Static PCC rules are bound to general purpose bearer with no Gx control.

A PCC rule consists of:

- **Rule Name:** The rule name is used to reference a PCC rule in the communication between the PCEF and PCRF.
- **Service Identifier:** The service identifier is used to identify the service or the service component the SDF relates to.
- **Service Data Flow Filter(s):** The service flow filter(s) is used to select the traffic for which the rule applies.
- **Precedence:** For different PCC rules with overlapping SDF filter, the precedence of the rule determines which of these rules is applicable. When a dynamic PCC rule and a predefined PCC rule have the same priority, the dynamic PCC rule takes precedence.
- **Gate Status:** The gate status indicates whether the SDF, detected by the SDF filter(s), may pass (gate is open) or will be discarded (gate is closed) in uplink and/or in downlink direction.
- **QoS Parameters:** The QoS information includes the QoS class identifier (authorized QoS class for the SDF), and authorized bitrates for uplink and downlink.
- **Charging Key (rating group)**
- **Other charging parameters:** The charging parameters define whether online charging interfaces are used, on what level the PCEF will report the usage related to the rule, etc.



**Important:** Configuring the Metering Method and Reporting Level for dynamic PCC rules is not supported.

PCC rules also include Application Function (AF) record information for enabling charging correlation between the application and bearer layer if the AF has provided this information via the Rx interface. For IMS, this includes the IMS Charging Identifier (ICID) and flow identifiers.

## PCC Procedures over Gx Reference Point

### Request for PCC Rules

The PCEF, via the Gx reference point, requests for PCC rules in the following instances:

- At IP-CAN session establishment
- At IP-CAN session modification

PCC rules can also be requested as a consequence of a failure in the PCC rule installation/activation or enforcement without requiring an event trigger.

### Provisioning of PCC Rules

The PCRF indicates, via the Rel. 8 Gx reference point, the PCC rules to be applied at the PCEF. This may be using one of the following procedures:

- PULL (provisioning solicited by the PCEF): In response to a request for PCC rules being made by the PCEF, the PCRF provisions PCC rules in the CC-Answer.
- PUSH (unsolicited provisioning): The PCRF may decide to provision PCC rules without obtaining a request from the PCEF. For example, in response to information provided to the PCRF via the Rx reference point, or in response to an internal trigger within the PCRF. To provision PCC rules without a request from the PCEF, the PCRF includes these PCC rules in an RA-Request message. No CCR/CCA messages are triggered by this RA-Request.


For each request from the PCEF or upon unsolicited provisioning, the PCRF provisions zero or more PCC rules. The PCRF may perform an operation on a single PCC rule by one of the following means:

- To activate or deactivate a PCC rule that is predefined at the PCEF, the PCRF provisions a reference to this PCC rule within a Charging-Rule-Name AVP and indicates the required action by choosing either the Charging-Rule-Install AVP or the Charging-Rule-Remove AVP.
- To install or modify a PCRF-provisioned PCC rule, the PCRF provisions a corresponding Charging-Rule-Definition AVP within a Charging-Rule-Install AVP.
- To remove a PCC rule which has previously been provisioned by the PCRF, the PCRF provisions the name of this rule as value of a Charging-Rule-Name AVP within a Charging-Rule-Remove AVP.

## Selecting a PCC Rule for Uplink IP Packets

If PCC is enabled, the PCEF selects the applicable PCC rule for each received uplink IP packet within an IP-CAN session by evaluating the packet against uplink SDF filters of PCRF-provided or predefined active PCC rules of this IP-CAN session in the order of the precedence of the PCC rules.

---

 **Important:** When a PCRF-provided PCC rule and a predefined PCC rule have the same precedence, the uplink SDF filters of the PCRF-provided PCC rule is applied first.


---

When a packet matches an SDF filter, the packet matching process for that packet is completed, and the PCC rule for that filter is applied. Uplink IP packets which do not match any PCC rule of the corresponding IP-CAN session are discarded.

## Selecting a PCC Rule for Downlink IP Packets

If PCC is enabled, the PCEF selects a PCC rule for each received downlink IP packet within an IP-CAN session by evaluating the packet against downlink SDF filters of PCRF-provided or predefined active PCC rules of the IP-CAN session in the order of precedence of the PCC rules.

---

 **Important:** When a PCRF-provided PCC rule and a predefined PCC rule have the same precedence, the downlink SDF filters of the PCRF-provided PCC rule are applied first.

---

When a packet matches an SDF filter, the packet matching process for that packet is completed, and the PCC rule for that filter is applied. Downlink IP packets that do not match any PCC rule of the IP-CAN session are discarded.

The following procedures are also supported:

- Indication of IP-CAN Session Termination: When the IP-CAN session is being terminated the PCEF contacts the PCRF.
- Request of IP-CAN Session Termination: If the PCRF decides to terminate an IP-CAN session due to an internal trigger or trigger from the SPR, the PCRF informs the PCEF. The PCEF acknowledges to the PCRF and



instantly removes/deactivates all the PCC rules that have been previously installed or activated on that IP-CAN session.

The PCEF applies IP-CAN specific procedures to terminate the IP-CAN session. The HA/PDSN sends a MIP Revocation Request with the teardown indicator set to indicate that the termination of the entire IP-CAN session is requested. Furthermore, the PCEF applies the “Indication of IP-CAN Session Termination” procedure.

- Use of the Supported-Features AVP during session establishment to inform the destination host about the required and optional features that the origin host supports.

## How it Works

This section describes how HA/PDSN Rel. 8 Gx Interface support works.

The following figure and table explain the IMS Authorization process between a system and IMS components that is initiated by the UE.

In this example, the Diameter Policy Control Application (DPCA) is the Gx interface to the PCRF. The interface between IMSA with PCRF is the Gx interface, and the interface between Session Manager (SessMgr) and Online Charging Service (OCS) is the Gy interface. Note that the IMSA service and DPCA are part of SessMgr on the system and separated in the figure for illustration purpose only.

Figure 44. HA/PDSN Rel. 8 Gx IMS Authorization Call Flow

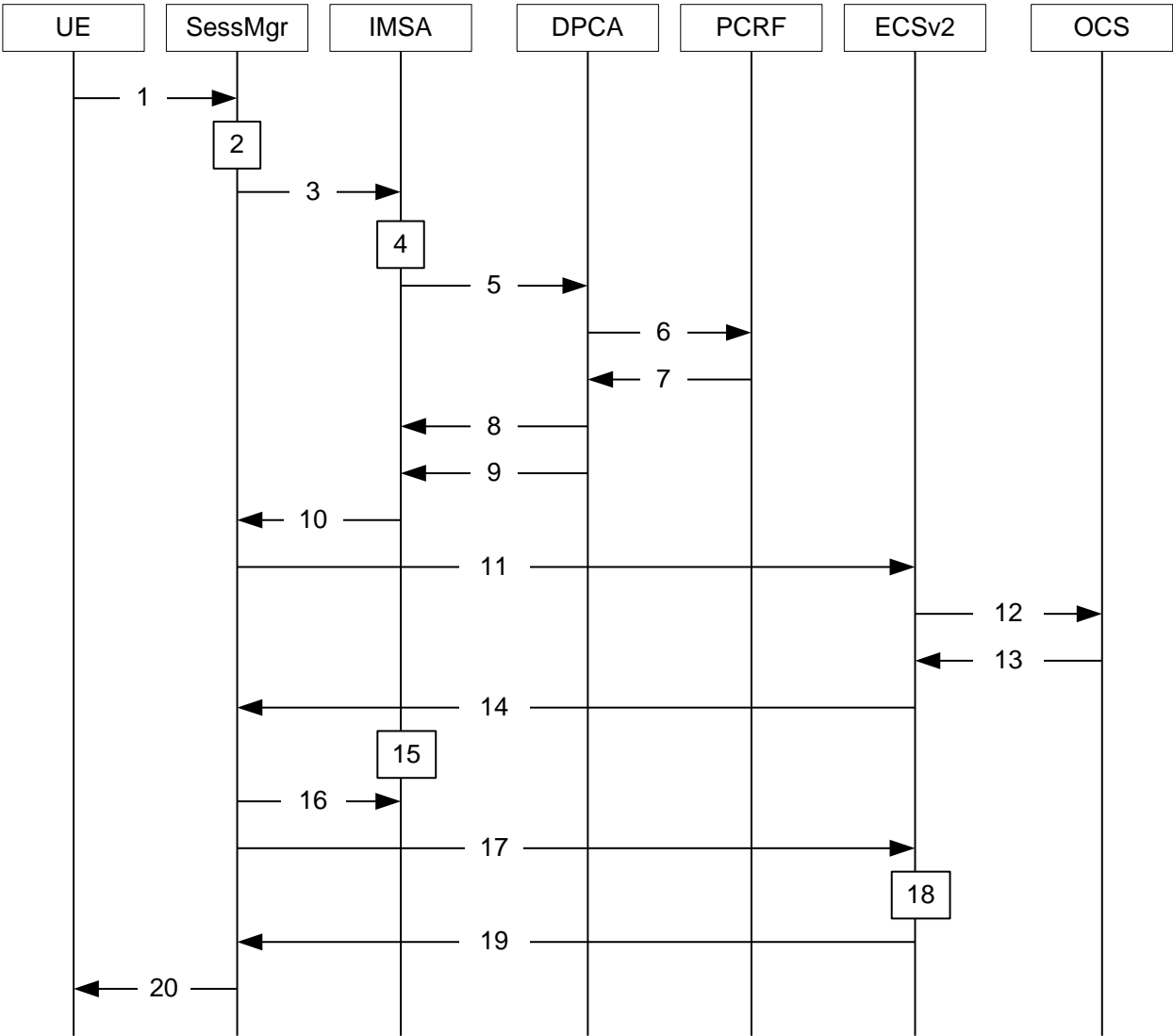


Table 19. HA/PDSN Rel. 8 Gx IMS Authorization Call flow Description

Step	Description
1	UE (IMS subscriber) requests for MIP Registration Request.
2	SessMgr allocates an IP address to the UE.
3	SessMgr requests IMS Authorization, if IMSA is enabled for the subscriber. IMSA service can either be configured in the subscriber template, or can be received from the AAA.
4	IMSA allocates resources for the IP-CAN session, and selects the PCRF to contact based on the user's selection key (for example, round-robin).
5	IMSA requests the DPCA module to issue an auth request to the PCRF.

Step	Description
6	DPCA sends a CCR initial message to the selected PCRF.
7	PCRF may send preconfigured charging rules in CCA. The dynamic rules and the authorized QoS parameters could also be included by the PCRF.
8	DPCA passes the charging rule definition, charging rule install, QoS information received from the PCRF, event triggers, etc. IMSA stores the information.
9	DPCA calls the callback function registered with it by IMSA.
10	PCRF-provided information common to the entire IP-CAN session (event trigger, primary/secondary OCS address, etc.) is stored within the IMSA. After processing the information, IMSA notifies the SessMgr about the policy authorization complete.
11	If the validation of the rules fails in IMSA/DPCA, a failure is notified to PCRF containing the Charging-Rule-Report AVP. Else, IMSA initiates creation of ECS session. The primary/secondary OCS server address, etc. are sent to the ECS from the SessMgr.
12	ECS performs credit authorization by sending CCR(I) to OCS with CC-Request-Type set to INITIAL_REQUEST to open the credit control session. This request includes the active Rulebase-Id (default rulebase ID from the AAA).
13	OCS returns a CCA initial message that may activate a statically configured Rulebase and may include preemptive quotas.
14	ECS responds to SessMgr with the response message.
15	SessMgr requests IMSA for the dynamic rules.
16	IMSA sends the dynamic rules to SessMgr. Note that until the MIP session is established, all RAR messages from the PCRF are rejected.
17	SessMgr sends the dynamic rule information to the ECS. The gate flow status information and the QoS per flow (charging rule) information are also sent in the message.
18	ECS activates the predefined rules received, and installs the dynamic rules received. Also, the gate flow status and the QoS parameters are updated by ECS as per the dynamic charging rules. The Gx rulebase is treated as an ECS group-of-ruledefs. The response message contains the Charging Rule Report conveying the status of the rule provisioning at the ECS.
19	If the provisioning of rules fails partially, the context setup is accepted, and a new CCR-U is sent to the PCRF with the Charging-Rule-Report containing the PCC rule status for the failed rules. If the provisioning of rules fails completely, the context setup is rejected.
20	Depending on the response for the MIP Session Authorization, SessMgr sends the response to the UE and activates/rejects the call. If the Charging-Rule-Report contains partial failure for any of the rules, the PCRF is notified, and the call is activated. If the Charging-Rule-Report contains complete failure, the call is rejected.

## Configuring HA/PDSN Rel. 8 Gx Interface Support

To configure HA/PDSN Rel. 8 Gx Interface functionality:

1. At the context level, configure IMSA service for IMS subscribers as described in the Configuring IMS Authorization Service at Context Level section.
2. Within the same context, configure the subscriber template to use the IMSA service as described in the Applying IMS Authorization Service to Subscriber Template section.

3. Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.



**Important:** Commands used in the configuration examples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the *Command Line Interface Reference* for complete information regarding all commands.

## Configuring IMS Authorization Service at Context Level

Use the following example to configure IMSA service at context level for IMS subscribers:

**configure**

```
context <context_name>

    ims-auth-service <imsa_service_name>

        policy-control

            diameter origin endpoint <endpoint_name>

            diameter dictionary <dictionary>

            diameter request-timeout <timeout_duration>

            diameter host-select table { 1 | 2 } algorithm round-robin

            diameter host-select row-precedence <precedence_value> table { 1 | 2 } host
<primary_host_name> [ realm <primary_realm_id> ] [ secondary host <secondary_host_name> [
realm <secondary_realm_id> ] ] [ -noconfirm ]

            failure-handling cc-request-type { any-request | initial-request | terminate-
request | update-request } { diameter-result-code { any-error | <result_code> [ to
<end_result_code> ] } } { continue | retry-and-terminate | terminate }

        exit

    exit

    diameter endpoint <endpoint_name> [ -noconfirm ]

        origin realm <realm_name>

        use-proxy

        origin host <host_name> address <ip_address>

        no watchdog-timeout

        response-timeout <timeout_duration>

        connection timeout <timeout_duration>
```

```

    connection retry-timeout <timeout_duration>

    peer <primary_peer_name> [ realm <primary_realm_name> ] address <ip_address> [
port <port_number> ]

    peer <secondary_peer_name> [ realm <secondary_realm_name> ] address <ip_address>
[ port <port_number> ]

end

```

#### Notes:

- <context\_name> must be the name of the context where you want to enable IMSA service.
- <imsa\_service\_name> must be the name of the IMSA service to be configured for Rel. 8 Gx interface authentication.
- A maximum of 16 authorization services can be configured globally in a system. There is also a system limit for the maximum number of total configured services.
- To enable Rel. 8 Gx interface support, pertinent Diameter dictionary must be configured. For information on the specific Diameter dictionary to use, please contact your local service representative.
- The Round Robin algorithm for PCRF selection is effective only over a large number of PCRF selections, and not at a granular level.
- To configure the PCRF host destinations configured in the PCEF, use the diameter host-select CLI commands.
- To configure the PCEF to use a pre-defined rule when the Gx fails, set the **failure-handling cc-request-type** CLI to **continue**. Policies available/in use will continue to be used and there will be no further interaction with the PCRF.

## Verifying the IMSA Service Configuration

To verify the IMSA service configuration:

- Change to the context where you enabled IMSA service by entering the following command:

```
context <context_name>
```
- Verify the IMSA service's configuration by entering the following command:

```
show ims-authorization service name <imsa_service_name>
```

## Applying IMS Authorization Service to Subscriber Template

After configuring IMSA service at the context-level, within the same context subscriber template must be configured to use the IMSA service for IMS subscribers.

Use the following example to apply IMSA service functionality to subscriber template within the context previously configured in the Configuring IMS Authorization Service at Context Level section.

```

configure

context <context_name>

    subscriber default

        encrypted password <encrypted_password>

        ims-auth-service <imsa_service_name>

```

```

ip access-group <access_group_name> in

ip access-group <access_group_name> out

ip context-name <context_name>

mobile-ip home-agent <ip_address>

active-charging rulebase <rulebase_name>

end

```

Notes:

- <context\_name> must be the name of the context in which the IMSA service was configured.
- <imsa\_service\_name> must be the name of the IMSA service configured for IMS authentication in the context.
- The ECS rulebase must be configured in the subscriber template.
- Provided interpretation of the Gx rulebase (Charging-Rule-Base-Name AVP) from PCRF is chosen to be ECS group-of-ruledefs, configure the following command in the Active Charging Service Configuration Mode:

```
policy-control charging-rule-base-name active-charging-group-of- ruledefs
```

## Verifying the Subscriber Configuration

Verify the IMSA service configuration for subscriber(s) by entering the following command in the Exec CLI configuration mode:

```
show subscribers ims-auth-service <imsa_service_name>
```

Notes:

<imsa\_service\_name> must be the name of the IMSA service configured for IMS authentication.

## Gathering Statistics

This section explains how to gather Rel. 8 Gx statistics and configuration information.

In the following table, the first column lists what statistics to gather, and the second column lists the action to perform.

Table 20. Gathering HA/PDSN Rel. 8 Gx Statistics and Information

Statistics/Information	Action to perform
Information and statistics specific to policy control in IMS Authorization service.	<b>show ims-authorization policy-control statistics</b>
Information and statistics specific to the authorization servers used for IMS Authorization service.	<b>show ims-authorization servers ims-auth-service</b>
Information of all IMS Authorization service.	<b>show ims-authorization service all</b>
Statistics of IMS Authorization service.	<b>show ims-authorization service statistics</b>
Information, configuration, and statistics of sessions active in IMS Authorization service.	<b>show ims-authorization sessions all</b>

Statistics/Information	Action to perform
Complete information, configuration, and statistics of sessions active in IMS Authorization service.	<code>show ims-authorization sessions full</code>
Summarized information of sessions active in IMS Authorization service.	<code>show ims-authorization sessions summary</code>
Complete statistics for active charging service sessions.	<code>show active-charging sessions full</code>
Information for all rule definitions configured in the service.	<code>show active-charging ruledef all</code>
Information for all rulebases configured in the system.	<code>show active-charging rulebase all</code>
Information on all group of ruledefs configured in the system.	<code>show active-charging group-of-ruledefs all</code>
Information on policy gate counters and status.	<code>show ims-authorization policy-gate { counters   status }</code>

## P-GW Rel. 8 Gx Interface Support

### Introduction

The Gx reference point is located between the Policy and Charging Rules Function (PCRF) and the Policy and Charging Enforcement Function (PCEF) on the Packet Data Network (PDN) Gateway (P-GW). The Gx reference point is used for provisioning and removal of PCC rules from the PCRF to the PCEF and the transmission of traffic plane events from the PCEF to the PCRF. The Gx reference point can be used for charging control, policy control, or both, by applying AVPs relevant to the application.

The PCEF is the functional element that encompasses policy enforcement and flow based charging functionality. This functional entity is located at the P-GW. The main functions include:

- Control over the user plane traffic handling at the gateway and its QoS.
- Service data flow detection and counting, as well as online and offline charging interactions.
- For a service data flow that is under policy control, the PCEF shall allow the service data flow to pass through the gateway if and only if the corresponding gate is open.
- For a service data flow that is under charging control, the PCEF shall allow the service data flow to pass through the gateway if and only if there is a corresponding active PCC rule and, for online charging, the OCS has authorized the applicable credit with that charging key.
- If requested by the PCRF, the PCEF shall report to the PCRF when the status of the related service data flow changes.
- In case the SDF is tunnelled at the BBERF, the PCEF shall inform the PCRF about the mobility protocol tunnelling header of the service data flows at IP-CAN session establishment.

### Terminology and Definitions

This section describes features and terminology pertaining to Rel. 8 Gx functionality.

### Volume Reporting Over Gx

This section describes the 3GPP Rel. 9 Volume Reporting over Gx feature.

## License Requirements

The Volume Reporting over Gx is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

## Supported Standards


The Volume Reporting over Gx feature is based on the following standard:

3GPP TS 29.212 V9.3.0 (2010-06): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control over Gx reference point (Release 9).


## Feature Overview


The Volume Reporting over Gx feature provides PCRF the capability to make real-time decisions based on the data usage by subscribers.

---

 **Important:** Volume Reporting over Gx is applicable only for volume quota.

 **Important:** In release 10.0, only total data usage reporting is supported, uplink/downlink level reporting is not supported. In 10.2 and later releases, it is supported.

 **Important:** The PCEF only reports the accumulated usage since the last report for usage monitoring and not from the beginning.

 **Important:** If the usage threshold is set to zero (infinite threshold), no further threshold events will be generated by PCEF, but monitoring of usage will continue and be reported at the end of the session.

 **Important:** In 12.2 and later releases, usage reporting on bearer termination is supported.

---

The following steps explain how Volume Reporting over Gx works:

1. PCEF after receiving the message from PCRF parses the usage monitoring related AVPs, and sends the information to IMSA.
2. IMSA updates the information to ECS.
3. Once the ECS is updated with the usage monitoring information from PCRF, the PCEF (ECS) starts tracking the data usage.
4. For session-level monitoring, the ECS maintains the amount of data usage.
5. For PCC rule monitoring, usage is monitored with the monitoring key as the unique identifier. Each node maintains the usage information per monitoring key. When the data traffic is passed, the usage is checked against the usage threshold values and reported as described in the *Usage Reporting* section.
6. The PCEF continues to track data usage after the threshold is reached and before a new threshold is provided by the PCRF. If a new usage threshold is not provided by the PCRF in the acknowledgement of an IP-CAN



Session modification where its usage was reported, then usage monitoring does not continue in the PCEF for that IP CAN session.

## Usage Monitoring

- **Usage Monitoring at Session Level:** PCRF subscribes to the session-level volume reporting over Gx by sending the Usage-Monitoring-Information AVP with the usage threshold level set in Granted-Service-Unit AVP and Usage-Monitoring-Level AVP set to SESSION\_LEVEL(0). After the AVPs are parsed by DPCA, IMSA updates the information to ECS. Once ECS is updated usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present. In 11.0 and later releases, Monitoring Key at session level is supported.

In 12.0 and later releases, enabling and disabling session usage in a single message from PCRF is supported. This is supported only if the monitoring key is associated at session level.

In 12.0 and later releases, monitoring of usage based on input/output octet threshold levels is supported. Usage is reported based on the enabled threshold level. If multiple levels are enabled, usage will be reported on all the enabled levels even if only one of the levels is breached. Monitoring will be stopped on the missing threshold levels in the response for the usage report from PCRF (expected to provide the complete set again if PCRF wants to continue monitoring on the multiple levels enabled earlier).

Total threshold level along with UL/DL threshold level in the GSU AVP is treated as an error and only total threshold level is accepted.

- **Usage Monitoring at Flow Level:** PCRF subscribes to the flow-level volume reporting over Gx by sending the Usage-Monitoring-Information AVP with the usage threshold level set in Granted-Service-Unit AVP and Usage-Monitoring-Level AVP set to PCC\_RULE\_LEVEL(1). Monitoring Key is mandatory in case of a flow-level monitoring since the rules are associated with the monitoring key and enabling/disabling of usage monitoring at flow level can be controlled by PCRF using it. After the AVPs are parsed by DPCA, IMSA updates the information to ECS. Once ECS is updated usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present.

Usage monitoring is supported for static, predefined rules, and dynamic rule definitions.

- **Usage Monitoring for Static Rules:** In the case of static rules, the usage reporting on last rule removal associated with the monitoring key is not applicable. In this case only the usage monitoring information is received from the PCRF.
- **Usage Monitoring for Predefined Rules:** If the usage monitoring needs to be enabled for the predefined rules, PCRF sends the rule and the usage monitoring information containing the monitoring key and the usage threshold. The Monitoring key should be same as the one pre-configured in PCEF for that predefined rule. There can be multiple rules associated with the same monitoring key. Hence enabling a particular monitoring key would result in the data being tracked for multiple rules having the same monitoring key. After DPCA parses the AVPs IMSA updates the information to ECS. Once ECS is updated usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present.
- **Usage Monitoring for Dynamic Rules:** If the usage monitoring needs to be enabled for dynamic ruledefs, PCRF provides the monitoring key along with a charging rule definition and the usage monitoring information containing the monitoring key and the usage threshold. This would result in the usage monitoring being done for all the rules associated with that monitoring key. After DPCA parses the AVPs, IMSA updates the information to ECS. Once ECS is updated, the usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present. Monitoring key for dynamic ruledef is dynamically assigned by PCRF which is the only difference with predefined rules in case of usage monitoring.

## Usage Reporting

Usage at subscriber/flow level is reported to PCRF under the following conditions:

- **Usage Threshold Reached:** PCEF records the subscriber data usage and checks if the usage threshold provided by PCRF is reached. This is done for both session and rule level reporting.

For session-level reporting, the actual usage volume is compared with the usage volume threshold.

For rule-level reporting the rule that hits the data traffic is used to find out if the monitoring key is associated with it, and based on the monitoring key the data usage is checked. Once the condition is met, it reports the usage information to IMSA and continues monitoring. IMSA then triggers the CCR-U if “USAGE\_REPORT” trigger is enabled by the PCRF. The Usage-Monitoring-Information AVP is sent in this CCR with the “Used-Service-Unit” set to the amount of data usage by subscriber.

If PCRF does not provide a new usage threshold in the usage monitoring information as a result of CCR from PCEF when the usage threshold is reached, the usage monitoring is stopped at PCEF and no usage status is reported.

In the non-standard Volume Reporting over Gx implementation, usage monitoring will be stopped once the threshold is breached, else the monitoring will continue. There will be no further usage reporting until the CCA is received.

- **Usage Monitoring Disabled:** If the PCRF explicitly disables the usage monitoring with Usage-Monitoring-Support AVP set to USAGE\_MONITORING\_DISABLED, the PCEF stops monitoring and reports the usage information (when the monitoring was enabled) to PCRF if the usage monitoring is disabled by PCRF as a result of CCR from PCEF which is not related to reporting usage, other external triggers, or a PCRF internal trigger. If the PCRF does not provide a new usage threshold as a result of CCR from PCEF when the usage threshold is reached, the usage monitoring is stopped at PCEF and no further usage status is reported.
- **IP CAN Session Termination:** When the IP CAN session is terminated, the accumulated subscriber usage information is reported to PCRF in the CCR-T from PCEF. If PCC usage level information is enabled by PCRF, the PCC usage will also be reported.
- **PCC Rule Removal:** When the PCRF deactivates the last PCC rule associated with a usage monitoring key, the PCEF sends a CCR with the data usage for that monitoring key. If the PCEF reports the last PCC rule associated with a usage monitoring key is inactive, the PCEF reports the accumulated usage for that monitoring key within the same CCR command if the Charging-Rule-Report AVP was included in a CCR command; otherwise, if the Charging-Rule-Report AVP was included in an RAA command, the PCEF sends a new CCR command to report accumulated usage for the usage monitoring key. In 12.0 and later releases, usage reporting on last rule deactivation using rule deactivation time set by PCRF is supported.
- **PCRF Requested Usage Report:** In 10.2 and later releases, the accumulated usage since the last report is sent even in case of immediate reporting, the usage is reset after immediate reporting and usage monitoring continued so that the subsequent usage report will have the usage since the current report. In earlier releases the behavior was to accumulate the so far usage in the next report.
- **Release 12.2 onwards,** usage reporting on bearer termination can be added. When a bearer is deleted due to some reason, the rules associated with the bearer will also be removed. So, the usage will be reported on the monitoring key(s) whose associated rule is the last one that is removed because of bearer termination.
- **Revalidation Timeout:** In the non-standard implementation, if usage monitoring and reporting is enabled and a revalidation timeout occurs, the PCEF sends a CCR to request PCC rules and reports all accumulated usage for all enabled monitoring keys since the last report (or since usage reporting was enabled if the usage was not yet reported) with the accumulated usage at IP-CAN session level (if enabled) and at service data flow level (if enabled) This is the default behavior.

In the case of standard implementation, this must be enabled by CLI configuration.



**Important:** The Usage Reporting on Revalidation Timeout feature is available by default in non-standard implementation of Volume Reporting over Gx. In 10.2 and later releases, this is configurable in the standard implementation. This is not supported in 10.0 release for standard based volume reporting.

Once the usage is reported, the usage counter is reset to zero. The PCEF continues to track data usage from the zero value after the threshold is reached and before a new threshold is provided by the PCRF. If a new usage threshold is not provided by the PCRF in the acknowledgement of an IP-CAN Session modification where its usage was reported, then usage monitoring does not continue in the PCEF for that IP CAN session and the usage accumulated between the CCR-CCA will be discarded.

For information on how to configure the Volume Reporting over Gx feature, see the [Configuring Volume Reporting over Gx](#) section.

# Rel. 9 Gx Interface

Rel. 9 Gx interface support is available on the Cisco ASR chassis running StarOS 12.2 and later releases.

## P-GW Rel. 9 Gx Interface Support

### Introduction

The Gx reference point is located between the Policy and Charging Rules Function (PCRF) and the Policy and Charging Enforcement Function (PCEF) on the Packet Data Network (PDN) Gateway (P-GW). The Gx reference point is used for provisioning and removal of PCC rules from the PCRF to the PCEF and the transmission of traffic plane events from the PCEF to the PCRF. The Gx reference point can be used for charging control, policy control, or both, by applying AVPs relevant to the application.

The PCEF is the functional element that encompasses policy enforcement and flow based charging functionality. This functional entity is located at the P-GW. The main functions include:

- Control over the user plane traffic handling at the gateway and its QoS.
- Service data flow detection and counting, as well as online and offline charging interactions.
- For a service data flow that is under policy control, the PCEF shall allow the service data flow to pass through the gateway if and only if the corresponding gate is open.
- For a service data flow that is under charging control, the PCEF shall allow the service data flow to pass through the gateway if and only if there is a corresponding active PCC rule and, for online charging, the OCS has authorized the applicable credit with that charging key.
- If requested by the PCRF, the PCEF shall report to the PCRF when the status of the related service data flow changes.
- In case the SDF is tunnelled at the BBERF, the PCEF shall inform the PCRF about the mobility protocol tunnelling header of the service data flows at IP-CAN session establishment.

### Terminology and Definitions

This section describes features and terminology pertaining to Rel. 9 Gx functionality.

### Volume Reporting Over Gx

This section describes the 3GPP Rel. 9 Volume Reporting over Gx feature.

### License Requirements

The Volume Reporting over Gx is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

### Supported Standards


The Volume Reporting over Gx feature is based on the following standard:


3GPP TS 29.212 V9.3.0 (2010-06): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control over Gx reference point (Release 9).


## Feature Overview


The Volume Reporting over Gx feature provides PCRF the capability to make real-time decisions based on the data usage by subscribers.


---

 **Important:** Volume Reporting over Gx is applicable only for volume quota.

 **Important:** In release 10.0, only total data usage reporting is supported, uplink/downlink level reporting is not supported. In 10.2 and later releases, it is supported.

 **Important:** The PCEF only reports the accumulated usage since the last report for usage monitoring and not from the beginning.

 **Important:** If the usage threshold is set to zero (infinite threshold), no further threshold events will be generated by PCEF, but monitoring of usage will continue and be reported at the end of the session.

 **Important:** In 12.2 and later releases, usage reporting on bearer termination is supported.

---

The following steps explain how Volume Reporting over Gx works:

1. PCEF after receiving the message from PCRF parses the usage monitoring related AVPs, and sends the information to IMSA.
2. IMSA updates the information to ECS.
3. Once the ECS is updated with the usage monitoring information from PCRF, the PCEF (ECS) starts tracking the data usage.
4. For session-level monitoring, the ECS maintains the amount of data usage.
5. For PCC rule monitoring, usage is monitored with the monitoring key as the unique identifier. Each node maintains the usage information per monitoring key. When the data traffic is passed, the usage is checked against the usage threshold values and reported as described in the *Usage Reporting* section.
6. The PCEF continues to track data usage after the threshold is reached and before a new threshold is provided by the PCRF. If a new usage threshold is not provided by the PCRF in the acknowledgement of an IP-CAN Session modification where its usage was reported, then usage monitoring does not continue in the PCEF for that IP CAN session.

## Usage Monitoring

- Usage Monitoring at Session Level: PCRF subscribes to the session-level volume reporting over Gx by sending the Usage-Monitoring-Information AVP with the usage threshold level set in Granted-Service-Unit AVP and Usage-Monitoring-Level AVP set to SESSION\_LEVEL(0). After the AVPs are parsed by DPCA, IMSA updates the information to ECS. Once ECS is updated usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present. In 11.0 and later releases, Monitoring Key at session level is supported.

In 12.0 and later releases, enabling and disabling session usage in a single message from PCRF is supported. This is supported only if the monitoring key is associated at session level.

In 12.0 and later releases, monitoring of usage based on input/output octet threshold levels is supported. Usage is reported based on the enabled threshold level. If multiple levels are enabled, usage will be reported on all the enabled levels even if only one of the levels is breached. Monitoring will be stopped on the missing threshold levels in the response for the usage report from PCRF (expected to provide the complete set again if PCRF wants to continue monitoring on the multiple levels enabled earlier).

Total threshold level along with UL/DL threshold level in the GSU AVP is treated as an error and only total threshold level is accepted.

- **Usage Monitoring at Flow Level:** PCRF subscribes to the flow-level volume reporting over Gx by sending the Usage-Monitoring-Information AVP with the usage threshold level set in Granted-Service-Unit AVP and Usage-Monitoring-Level AVP set to PCC\_RULE\_LEVEL(1). Monitoring Key is mandatory in case of a flow-level monitoring since the rules are associated with the monitoring key and enabling/disabling of usage monitoring at flow level can be controlled by PCRF using it. After the AVPs are parsed by DPCA, IMSA updates the information to ECS. Once ECS is updated usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present.

Usage monitoring is supported for static, predefined rules, and dynamic rule definitions.

- **Usage Monitoring for Static Rules:** In the case of static rules, the usage reporting on last rule removal associated with the monitoring key is not applicable. In this case only the usage monitoring information is received from the PCRF.
- **Usage Monitoring for Predefined Rules:** If the usage monitoring needs to be enabled for the predefined rules, PCRF sends the rule and the usage monitoring information containing the monitoring key and the usage threshold. The Monitoring key should be same as the one pre-configured in PCEF for that predefined rule. There can be multiple rules associated with the same monitoring key. Hence enabling a particular monitoring key would result in the data being tracked for multiple rules having the same monitoring key. After DPCA parses the AVPs IMSA updates the information to ECS. Once ECS is updated usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present.
- **Usage Monitoring for Dynamic Rules:** If the usage monitoring needs to be enabled for dynamic ruledefs, PCRF provides the monitoring key along with a charging rule definition and the usage monitoring information containing the monitoring key and the usage threshold. This would result in the usage monitoring being done for all the rules associated with that monitoring key. After DPCA parses the AVPs, IMSA updates the information to ECS. Once ECS is updated, the usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present. Monitoring key for dynamic ruledef is dynamically assigned by PCRF which is the only difference with predefined rules in case of usage monitoring.

## Usage Reporting

Usage at subscriber/flow level is reported to PCRF under the following conditions:

- **Usage Threshold Reached:** PCEF records the subscriber data usage and checks if the usage threshold provided by PCRF is reached. This is done for both session and rule level reporting.

For session-level reporting, the actual usage volume is compared with the usage volume threshold.

For rule-level reporting the rule that hits the data traffic is used to find out if the monitoring key is associated with it, and based on the monitoring key the data usage is checked. Once the condition is met, it reports the usage information to IMSA and continues monitoring. IMSA then triggers the CCR-U if “USAGE\_REPORT” trigger is enabled by the PCRF. The Usage-Monitoring-Information AVP is sent in this CCR with the “Used-Service-Unit” set to the amount of data usage by subscriber.

If PCRF does not provide a new usage threshold in the usage monitoring information as a result of CCR from PCEF when the usage threshold is reached, the usage monitoring is stopped at PCEF and no usage status is reported.

In the non-standard Volume Reporting over Gx implementation, usage monitoring will be stopped once the threshold is breached, else the monitoring will continue. There will be no further usage reporting until the CCA is received.

- **Usage Monitoring Disabled:** If the PCRF explicitly disables the usage monitoring with Usage-Monitoring-Support AVP set to `USAGE_MONITORING_DISABLED`, the PCEF stops monitoring and reports the usage information (when the monitoring was enabled) to PCRF if the usage monitoring is disabled by PCRF as a result of CCR from PCEF which is not related to reporting usage, other external triggers, or a PCRF internal trigger. If the PCRF does not provide a new usage threshold as a result of CCR from PCEF when the usage threshold is reached, the usage monitoring is stopped at PCEF and no further usage status is reported.
- **IP CAN Session Termination:** When the IP CAN session is terminated, the accumulated subscriber usage information is reported to PCRF in the CCR-T from PCEF. If PCC usage level information is enabled by PCRF, the PCC usage will also be reported.
- **PCC Rule Removal:** When the PCRF deactivates the last PCC rule associated with a usage monitoring key, the PCEF sends a CCR with the data usage for that monitoring key. If the PCEF reports the last PCC rule associated with a usage monitoring key is inactive, the PCEF reports the accumulated usage for that monitoring key within the same CCR command if the Charging-Rule-Report AVP was included in a CCR command; otherwise, if the Charging-Rule-Report AVP was included in an RAA command, the PCEF sends a new CCR command to report accumulated usage for the usage monitoring key. In 12.0 and later releases, usage reporting on last rule deactivation using rule deactivation time set by PCRF is supported.
- **PCRF Requested Usage Report:** In 10.2 and later releases, the accumulated usage since the last report is sent even in case of immediate reporting, the usage is reset after immediate reporting and usage monitoring continued so that the subsequent usage report will have the usage since the current report. In earlier releases the behavior was to accumulate the so far usage in the next report.
- **Release 12.2 onwards,** usage reporting on bearer termination can be added. When a bearer is deleted due to some reason, the rules associated with the bearer will also be removed. So, the usage will be reported on the monitoring key(s) whose associated rule is the last one that is removed because of bearer termination.
- **Revalidation Timeout:** In the non-standard implementation, if usage monitoring and reporting is enabled and a revalidation timeout occurs, the PCEF sends a CCR to request PCC rules and reports all accumulated usage for all enabled monitoring keys since the last report (or since usage reporting was enabled if the usage was not yet reported) with the accumulated usage at IP-CAN session level (if enabled) and at service data flow level (if enabled) This is the default behavior.

In the case of standard implementation, this must be enabled by CLI configuration.



**Important:** The Usage Reporting on Revalidation Timeout feature is available by default in non-standard implementation of Volume Reporting over Gx. In 10.2 and later releases, this is configurable in the standard implementation. This is not supported in 10.0 release for standard based volume reporting.

Once the usage is reported, the usage counter is reset to zero. The PCEF continues to track data usage from the zero value after the threshold is reached and before a new threshold is provided by the PCRF. If a new usage threshold is not provided by the PCRF in the acknowledgement of an IP-CAN Session modification where its usage was reported, then usage monitoring does not continue in the PCEF for that IP CAN session and the usage accumulated between the CCR-CCA will be discarded.

For information on how to configure the Volume Reporting over Gx feature, see the [Configuring Volume Reporting over Gx](#) section.





# Appendix D

## Gy Interface Support

---

This chapter provides an overview of the Gy interface and describes how to configure the Gy interface.

Gy interface support is available on the Cisco system running StarOS 9.0 or later releases for the following products:

- GGSN
- HA
- IPSP
- PDSN
- P-GW

It is recommended that before using the procedures in this chapter you select the configuration example that best meets your service model, and configure the required elements for that model as described in the administration guide for the product that you are deploying.

This chapter describes the following topics:

- [Introduction](#)
- [Features and Terminology](#)
- [Configuring Gy Interface Support](#)

# Introduction

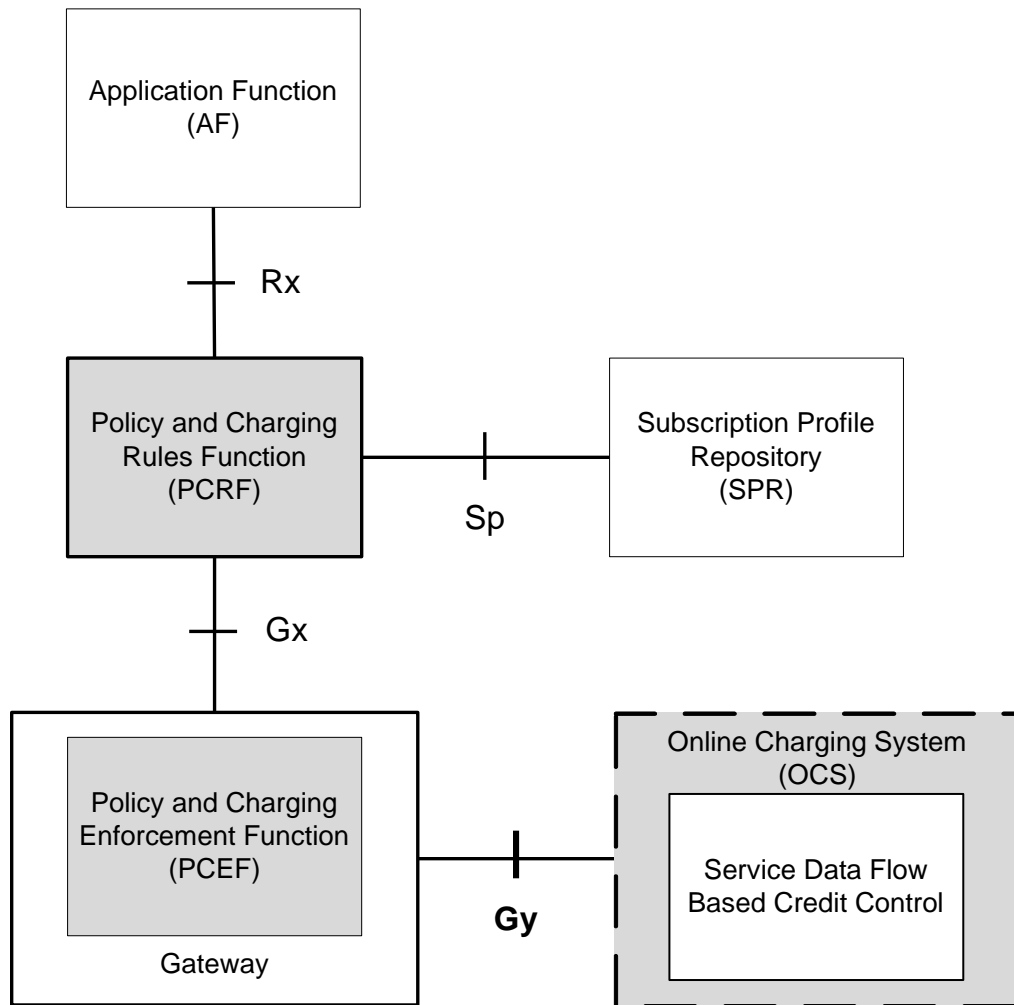
The Gy interface is the online charging interface between the PCEF/GW (Charging Trigger Function (CTF)) and the Online Charging System (Charging-Data-Function (CDF)).

The Gy interface makes use of the Active Charging Service (ACS) / Enhanced Charging Service (ECS) for real-time content-based charging of data services. It is based on the 3GPP standards and relies on quota allocation. The Online Charging System (OCS) is the Diameter Credit Control server, which provides the online charging data to the PCEF/GW. With Gy, customer traffic can be gated and billed in an online or prepaid style. Both time- and volume-based charging models are supported. In these models differentiated rates can be applied to different services based on ECS shallow- or deep-packet inspection.

In the simplest possible installation, the system will exchange Gy Diameter messages over Diameter TCP links between itself and one prepay server. For a more robust installation, multiple servers would be used. These servers may optionally share or mirror a single quota database so as to support Gy session failover from one server to the other. For a more scalable installation, a layer of proxies or other Diameter agents can be introduced to provide features such as multi-path message routing or message and session redirection features.

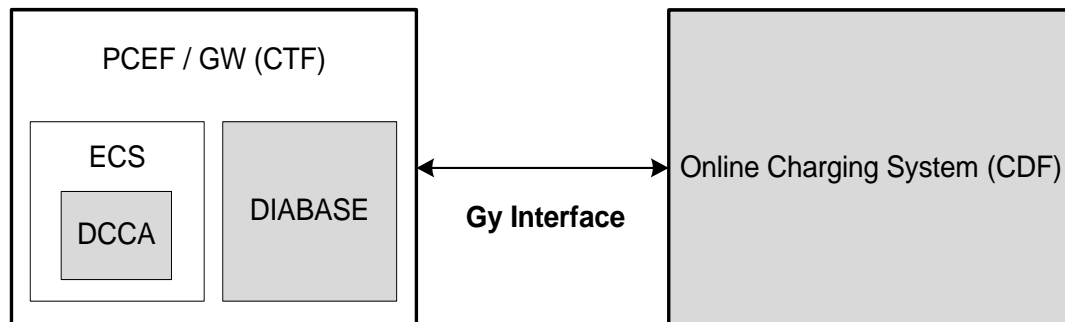
The following figure shows the Gy reference point in the policy and charging architecture.

Figure 45. PCC Logical Architecture



The following figure shows the Gy interface between CTF/Gateway/PCEF/Client running ECS and OCS (CDF/Server). Within the PCEF/GW, the Gy protocol functionality is handled in the DCCA module (at the ECS).

Figure 46. Gy Architecture



## License Requirements

The Gy interface support is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

## Supported Standards

Gy interface support is based on the following standards:


- IETF RFC 4006: Diameter Credit Control Application; August 2005
- 3GPP TS 32.299 V9.6.0 (2010-12) 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Charging management; Diameter charging applications (Release 9)

# Features and Terminology

This section describes features and terminology pertaining to Gy functionality.

## Charging Scenarios

---

 **Important:** Online charging for events (“Immediate Event Charging” and “Event Charging with Reservation”) is not supported. Only “Session Charging with Reservation” is supported.

---

### Session Charging with Reservation

Session Charging with Unit Reservation is used for credit control of sessions.

### Decentralized Unit Determination and Centralized Rating


In this scenario, the CTF requests the reservation of units prior to session supervision. An account debit operation is carried out following the conclusion of session termination.

### Centralized Unit Determination and Centralized Rating

In this scenario, the CTF requests the OCS to reserve units based on the session identifiers specified by the CTF. An account debit operation is carried out following the conclusion of session.

### Decentralized Unit Determination and Decentralized Rating

---


 **Important:** Decentralized Rating is not supported in this release. Decentralized Unit determination is done using CLI configuration.

---

In this scenario, the CTF requests the OCS to assure the reservation of an amount of the specified number of monetary units from the subscriber's account. An account debit operation that triggers the deduction of the amount from the subscriber's account is carried out following the conclusion of session establishment.

## Basic Operations

---

 **Important:** Immediate Event Charging is not supported in this release. “Reserve Units Request” and “Reserve Units Response” are done for Session Charging and not for Event Charging.

---

Online credit control uses the basic logical operations “Debit Units” and “Reserve Units”.

- **Debit Units Request;** sent from CTF to OCS: After receiving a service request from the subscriber, the CTF sends a Debit Units Request to the OCS. The CTF may either specify a service identifier (centralised unit determination) or the number of units requested (decentralised unit determination). For refund purpose, the CTF sends a Debit Units Request to the OCS as well.

- Debit Units Response; sent from OCS to CTF: The OCS replies with a Debit Units Response, which informs the CTF of the number of units granted as a result of the Debit Units Request. This includes the case where the number of units granted indicates the permission to render the requested service. For refund purpose, the OCS replies with a Debit Units Response.
- Reserve Units Request; sent from CTF to OCS: Request to reserve a number of units for the service to be provided by an CTF. In case of centralised unit determination, the CTF specifies a service identifier in the Reserve Unit Request, and the OCS determines the number of units requested. In case of decentralised unit determination, the number of units requested is specified by the CTF.
- Reserve Units Response; sent from OCS to CTF: Response from the OCS which informs the CTF of the number of units that were reserved as a result of the “Reserve Units Request”.

Session Charging with Unit Reservation (SCUR) use both the “Debit Units” and “Reserve Units” operations. SCUR uses the Session Based Credit Control procedure specified in RFC 4006. In session charging with unit reservation, when the “Debit Units” and “Reserve Units” operations are both needed, they are combined in one message.



**Important:** Cost-Information, Remaining-Balance, and Low-Balance-Indication AVPs are not supported.

The consumed units are deducted from the subscriber's account after service delivery. Thus, the reserved and consumed units are not necessarily the same. Using this operation, it is also possible for the CTF to modify the current reservation, including the return of previously reserved units.

## Re-authorization

The server may specify an idle timeout associated with a granted quota. Alternatively, the client may have a configurable default value. The expiry of that timer triggers a re-authorization request.

Mid-session service events (re-authorization triggers) may affect the rating of the current service usage. The server may instruct the credit control client to re-authorize the quota upon a number of different session related triggers that can affect the rating conditions.

When a re-authorization is trigger, the client reports quota usage. The reason for the quota being reported is notified to the server.

## Threshold based Re-authorization Triggers

The server may optionally include an indication to the client of the remaining quota threshold that triggers a quota re-authorization.

## Termination Action

The server may specify to the client the behavior on consumption of the final granted units; this is known as termination action.

## Diameter Base Protocol

The Diameter Base Protocol maintains the underlying connection between the Diameter Client and the Diameter Server. The connection between the client and server is TCP based. There are a series of message exchanges to check the status of the connection and the capabilities.

- **Capabilities Exchange Messages:** Capabilities Exchange Messages are exchanged between the diameter peers to know the capabilities of each other and identity of each other.
  - **Capabilities Exchange Request (CER):** This message is sent from the client to the server to know the capabilities of the server.
  - **Capabilities Exchange Answer (CEA):** This message is sent from the server to the client in response to the CER message.



**Important:** Acct-Application-Id is not parsed and if sent will be ignored by the PCEF/GW. In case the Result-Code is not DIAMETER\_SUCCESS, the connection to the peer is closed.

- **Device Watchdog Request (DWR):** After the CER/CEA messages are exchanged, if there is no more traffic between peers for a while, to monitor the health of the connection, DWR message is sent from the client. The Device Watchdog timer (Tw) is configurable in PCEF/GW and can vary from 6 through 30 seconds. A very low value will result in duplication of messages. The default value is 30 seconds. On two consecutive expiries of Tw without a DWA, the peer is taken to be down.



**Important:** DWR is sent only after Tw expiry after the last message that came from the server. Say if there is continuous exchange of messages between the peers, DWR might not be sent if (Current Time - Last message received time from server) is less than Tw.

- **Device Watchdog Answer (DWA):** This is the response to the DWR message from the server. This is used to monitor the connection state.
- **Disconnect Peer Request (DPR):** This message is sent to the peer to inform to shutdown the connection. PCEF/GW only receives this message. There is no capability currently to send the message to the diameter server.
- **Disconnect Peer Answer (DPA):** This message is the response to the DPR request from the peer. On receiving the DPR, the peer sends DPA and puts the connection state to “DO NOT WANT TO TALK TO YOU” state and there is no way to get the connection back except for reconfiguring the peer again.  
A timeout value for retrying the disconnected peer must be provided.
- **Tw Timer Expiry Behavior:** The connection between the client and the server is taken care by the DIABASE application. When two consecutive Tw timers are expired, the peer state is set to idle and the connection is retried to be established. All the active sessions on the connection are then transferred to the secondary connection if one is configured. All new session activations are also tried on the secondary connection.  
There is a connection timeout interval, which is also equivalent to Tw timer, wherein after a CER has been sent to the server, if there is no response received while trying to reestablish connection, the connection is closed and the state set to idle.

## Diameter Credit Control Application

The Diameter Credit Control Application (DCCA) is a part of the ECS subsystem. For every prepaid customer with Diameter Credit Control enabled, whenever a session comes up, the Diameter server is contacted and quota for the subscriber is fetched.

## Quota Behavior

Various forms of quotas are present that can be used to charge the subscriber in an efficient way. Various quota mechanisms provide the end user with a variety of options to choose from and better handling of quotas for the service provider.

## Time Quotas

The Credit-Control server can send the CC-Time quota for the subscriber during any of the interrogation of client with it. There are also various mechanisms as discussed below which can be used in conjunction with time quota to derive variety of methods for customer satisfaction.

- **Quota Consumption Time:** The server can optionally indicate to the client that the quota consumption must be stopped after a period equal to the “Quota Consumption Time” in which no packets are received or at session termination, whichever is sooner. The idle period equal to the Quota Consumption Time is included in the reported usage. The quota is consumed normally during gaps in traffic of duration less than or equal to the Quota-Consumption-Time. Quota consumption resumes on receipt of a further packet belonging to the service data flow.

If packets are allowed to flow during a CCR (Update)/CCA exchange, and the Quota-Consumption-Time AVP value in the provided quota is the same as in the previously provided quota, then the Quota-Consumption-Time runs normally through this procedure. For example, if 5 seconds of a 10 second QCT timer have passed when a CCR(U) is triggered, and the CCA(U) returns 2 seconds later, then the QCT timer will expire 3 seconds after the receipt of the CCA and the remaining unaccounted 5 seconds of usage will be recorded against the new quota even though no packets were transmitted with the new quota.

A locally configurable default value in the client can be used if the server doesn't send the QCT in the CCA.

- **Combinational Quota:** Discrete-Time-Period (DTP) and Continuous-Time-Period (CTP) defines mechanisms that extends and generalize the Quota-Consumption-Time for consuming time-quota.
  - Both DTP and CTP uses a “base-time-interval” that is used to create time-envelopes of quota used.
  - Instead of consuming the quota linearly, DTP and CTP consumes the granted quota discretely in chunks of base-time-interval at the start of the each base-time-interval.
  - Selection of one of this algorithm is based on the “Time-Quota-Mechanism” AVP sent by the server in CCA.
  - Reporting usage can also be controlled by Envelope-Reporting AVP sent by the server in CCA during the quota grant. Based on the value of this AVP, the usage can be reported either as the usage per envelope or as usual cumulative usage for that grant.
- **Discrete-Time-Period:** The base-time-interval defines the length of the Discrete-Time-Period. So each time-envelope corresponds to exactly one Discrete-Time-Period. So when a traffic is detected, an envelope of size equal to Base-Time-Interval is created. The traffic is allowed to pass through the time-envelope. Once the traffic exceeds the base-time-interval another new envelope equal to the base-time-interval is created. This continues till the quota used exceeds the quota grant or reaches the threshold limit for that quota.
- **Continuous-Time-Period:** Continuous time period mechanism constructs time envelope out of consecutive base-time intervals in which the traffic occurred up to and including a base time interval which contains no traffic. Therefore the quota consumption continues within the time envelope, if there was traffic in the previous base time interval. After an envelope has closed, then the quota consumption resumes only on the first traffic following the closure of the envelope. The envelope for CTP includes the last base time interval which contains no traffic.

The size of the envelope is not constant as it was in Parking meter. The end of the envelope can only be determined retrospectively.



- **Quota Hold Time:** The server can specify an idle timeout associated with a granted quota using the Quota-Holding-Time AVP. If no traffic associated with the quota is observed for this time, the client understands that the traffic has stopped and the quota is returned to the server. The client starts the quota holding timer when quota consumption ceases. This is always when traffic ceases, i.e. the timer is re-started at the end of each packet. It applies equally to the granted time quota and to the granted volume quota. The timer is stopped on sending a CCR and re-initialized on receiving a CCA with the previous used value or a new value of Quota-Holding-Time if received.

Alternatively, if this AVP is not present, a locally configurable default value in the client is used. A Quota-Holding-Time value of zero indicates that this mechanism is not used.

- **Quota Validity Time:** The server can optionally send the validity time for the quota during the interrogation with the client. The Validity-Time AVP is present at the MSCC level and applies equally to the entire quota that is present in that category. The quota gets invalidated at the end of the validity time and a CCR-Update is sent to the server with the Used-Service-Units AVP and the reporting reason as VALIDITY\_TIME. The entire quota present in that category will be invalidated upon Quota-Validity-Time expiry and traffic in that category will be passed or dropped depending on the configuration, till a CCA-Update is received with quota for that category.

Validity-Time of zero is invalid. Validity-Time is relative and not absolute.

## Volume Quota

The server sends the CC-Total-Octets AVP to provide volume quota to the subscriber. DCCA currently supports only CC-Total-Octets AVP, which applies equally to uplink and downlink packets. If the total of uplink and downlink packets exceeds the CC-Total-Octets granted, the quota is assumed to be exhausted.

If CC-Input-Octets and/or CC-Output-Octets is provided, the quota is counted against CC-Input-Octets and/or CC-Output-Octets respectively.



**Important:** Restricting usages based on CC-Input-Octets and CC\_Output-Octets is not supported in this release.

## Units Quota

The server can also send a CC-Service-Specific-Units quota which is used to have packets counted as units. The number of units per packet is a configurable option.

## Granting Quota

Gy implementation assumes that whenever the CC-Total-Octets AVP is present, volume quota has been granted for both uplink and downlink.

If the Granted-Service-Unit contains no data, Gy treats it as an invalid CCA.

If the values are zero, it is assumed that no quota was granted.

If the AVP contains the sub AVPs without any data, it is assumed to be infinite quota.

Additional parameters relating to a category like QHT, QCT is set for the category after receiving a valid volume or time grant.

If a default quota is configured for the subscriber, and subscriber traffic is received it is counted against the default quota. The default quota is applicable only to the initial request and is not regranted during the course of the session. If subscriber disconnects and reconnects, the default quota will be applied again for the initial request.

## Requesting Quota

Quotas for a particular category type can be requested using the Requested-Service-Unit AVP in the CCR. The MSCC is filled with the Rating-Group AVP which corresponds to the category of the traffic and Requested-Service-Unit AVP without any data.

The Requested-Service-Unit can contain the CC AVPs used for requesting specific quantity of time or volume grant. Gy CLI can be used to request quota for a category type.

Alternatively quota can also be requested from the server preemptively for a particular category in CCR- I. When the server grants preemptive quota through the Credit control answer response, the quota will be used only when traffic is hit for that category. Quota can be preemptively requested from the Credit Control server from the CLI.

## Reporting Quota

Quotas are reported to the server for number of reasons including:

- Threshold
- QHT Expiry
- Quota Exhaustion
- Rating Condition Change
- Forced Reauthorization
- Validity Time Expiry
- Final during Termination of Category Instance from Server

For the above cases except for QHT and Final, the Requested-Service-Unit AVP is present in the CCR.

Reporting Reason is present in CCR to let the server know the reason for the reporting of Quota. The Reporting-Reason AVP can be present either in MSCC level or at Used Service Unit (USU) level depending on whether the reason applies to all quotas or to single quota.

When one of these conditions is met, a CCR Update is sent to the server containing a Multiple-Services-Credit-Control AVP(s) indicating the reason for reporting usage in the Reporting-Reason and the appropriate value(s) for Trigger, where appropriate. Where a threshold was reached, the DCCA still has the amount of quota available to it defined by the threshold.

For all other reporting reasons the client discards any remaining quota and either discards future user traffic matching this category or allows user traffic to pass, or buffers traffic according to configuration.

For Reporting-Reason of Rating Condition Change, Gy requires the Trigger Type AVP to be present as part of the CCR to indicate which trigger event caused the reporting and re-authorization request.

For Reporting-Reason of end user service denied, this happens when a category is blacklisted by the credit control server, in this case a CCR-U is sent with used service unit even if the values as zero. When more quota is received from the server for that particular category, the blacklisting is removed.

If a default quota has been set for the subscriber then the usage from the default quota is deducted from the initial GSU received for the subscriber for the Rating Group or Rating Group and Service ID combination.

## Default Quota Handling

- If default quota is set to 0, no data is passed/reported.
- If default quota is configured and default quota is not exhausted before OCS responds with quota, traffic is passed. Initial default quota used is counted against initial quota allocated. If quota allocated is less than the actual usage then actual usage is reported and additional quota requested. If no additional quota is available then traffic is denied.

- If default quota is not exhausted before OCS responds with denial of quota, gateway blocks traffic after OCS response. Gateway will report usage on default quota even in this case in CCR-U (FINAL) or CCR-T.
- if default quota is consumed before OCS responds, if OCS is not declared dead (see definition in use case 1 above) then traffic is blocked until OCS responds.

## Thresholds

The Gy client supports the following threshold types:

- Volume-Quota-Threshold
- Time-Quota-Threshold
- Units-Quota-Threshold

A threshold is always associated with a particular quota and a particular quota type. In the Multiple-Services-Credit-Control AVP, the Time-Quota-Threshold, Volume-Quota-Threshold, and Unit-Quota-Threshold are optional AVPs.

They are expressed as unsigned numbers and the units are seconds for time quota, octets for volume quota and units for service specific quota. Once the quota has reached its threshold, a request for more quotas is triggered toward the server. User traffic is still allowed to flow. There is no disruption of traffic as the user still has valid quota.

The Gy sends a CCR Update with a Multiple-Services-Credit-Control AVP containing usage reported in one or more User-Service-Unit AVPs, the Reporting-Reason set to THRESHOLD and the Requested-Service-Unit AVP without data.

When quota of more than one type has been assigned to a category, each with its own threshold, then the threshold is considered to be reached once one of the unit types has reached its threshold even if the other unit type has not been consumed.

When reporting volume quota, the DCCA always reports uplink and downlink separately using the CC-Input-Octets AVP and the CC-Output-Octets AVP, respectively.

On receipt of more quotas in the CCA the Gy discards any quota not yet consumed since sending the CCR. Thus the amount of quota now available for consumption is the new amount received less any quota that may have been consumed since last sending the CCR.

## Conditions for Reauthorization of Quota

Quota is re-authorized/requested from the server in case of the following scenarios:

- Threshold is hit
- Quota is exhausted
- Validity time expiry
- Rating condition change:
  - Cellid change: Applicable only to GGSN and P-GW implementations.
  - LAC change: Applicable only to GGSN and P-GW implementations.
  - QoS change
  - RAT change
  - SGSN/Serving-Node change: Applicable only to GGSN and P-GW implementations.

## Discarding or Allowing or Buffering Traffic to Flow

Whenever Gy is waiting for CCA from the server, there is a possibility of traffic for that particular traffic type to be encountered in the Gy. The behavior of what needs to be done to the packet is determined by the configuration. Based on the configuration, the traffic is either allowed to pass or discarded or buffered while waiting for CCA from the server.

This behavior applies to all interrogation of client with server in the following cases:

- No quota present for that particular category
- Validity timer expiry for that category
- Quota exhausted for that category
- Forced Reauthorization from the server

In addition to allowing or discarding user traffic, there is an option available in case of quota exhausted or no quota circumstances to buffer the traffic. This typically happens when the server has been requested for more quota, but a valid quota response has not been received from the server, in this case the user traffic is buffered and on reception of valid quota response from the server the buffered traffic is allowed to pass through.

## Procedures for Consumption of Time Quota

- QCT is zero: When QCT is deactivated, the consumption is on a wall-clock basis. The consumption is continuous even if there is no packet flow.
- QCT is active: When QCT is present in the CCA or locally configured for the session, then the consumption of quota is started only at the time of first packet arrival. The quota is consumed normally till last packet arrival plus QCT time and is passed till the next packet arrival.  
If the QCT value is changed during intermediate interrogations, then the new QCT comes into effect from the time the CCA is received. For instance, if the QCT is deactivated in the CCA, then quota consumptions resume normally even without any packet flow. Or if the QCT is activated from deactivation, then the quota consumption resume only after receiving the first packet after CCA.
- QHT is zero: When QHT is deactivated, the user holds the quota indefinitely in case there is no further usage (for volume quota and with QCT for time quota). QHT is active between the CCA and the next CCR.
- QHT is non-zero: When QHT is present in CCA or locally configured for the session, then after a idle time of QHT, the quota is returned to the server by sending a CCR-Update and reporting usage of the quota. On receipt of CCR-U, the server does not grant quota. QHT timer is stopped on sending the CCR and is restarted only if QHT is present in the CCA.  
QHT timer is reset every time a packet arrives.

## Envelope Reporting

The server may determine the need for additional detailed reports identifying start time and end times of specific activity in addition to the standard quota management. The server controls this by sending a CCA with Envelope-Reporting AVP with the appropriate values. The DCCA client, on receiving the command, will monitor for traffic for a period of time controlled by the Quota-Consumption-Time AVP and report each period as a single envelope for each Quota-Consumption-Time expiry where there was traffic. The server may request envelope reports for just time or time and volume. Reporting the quota back to the server, is controlled by Envelope AVP with Envelope-Start-Time and Envelope-End-Time along with usage information.

## Credit Control Request

Credit Control Request (CCR) is the message that is sent from the client to the server to request quota and authorization. CCR is sent before the establishment of MIP session, and at the termination of the MIP session. It can be sent during service delivery to request more quotas.

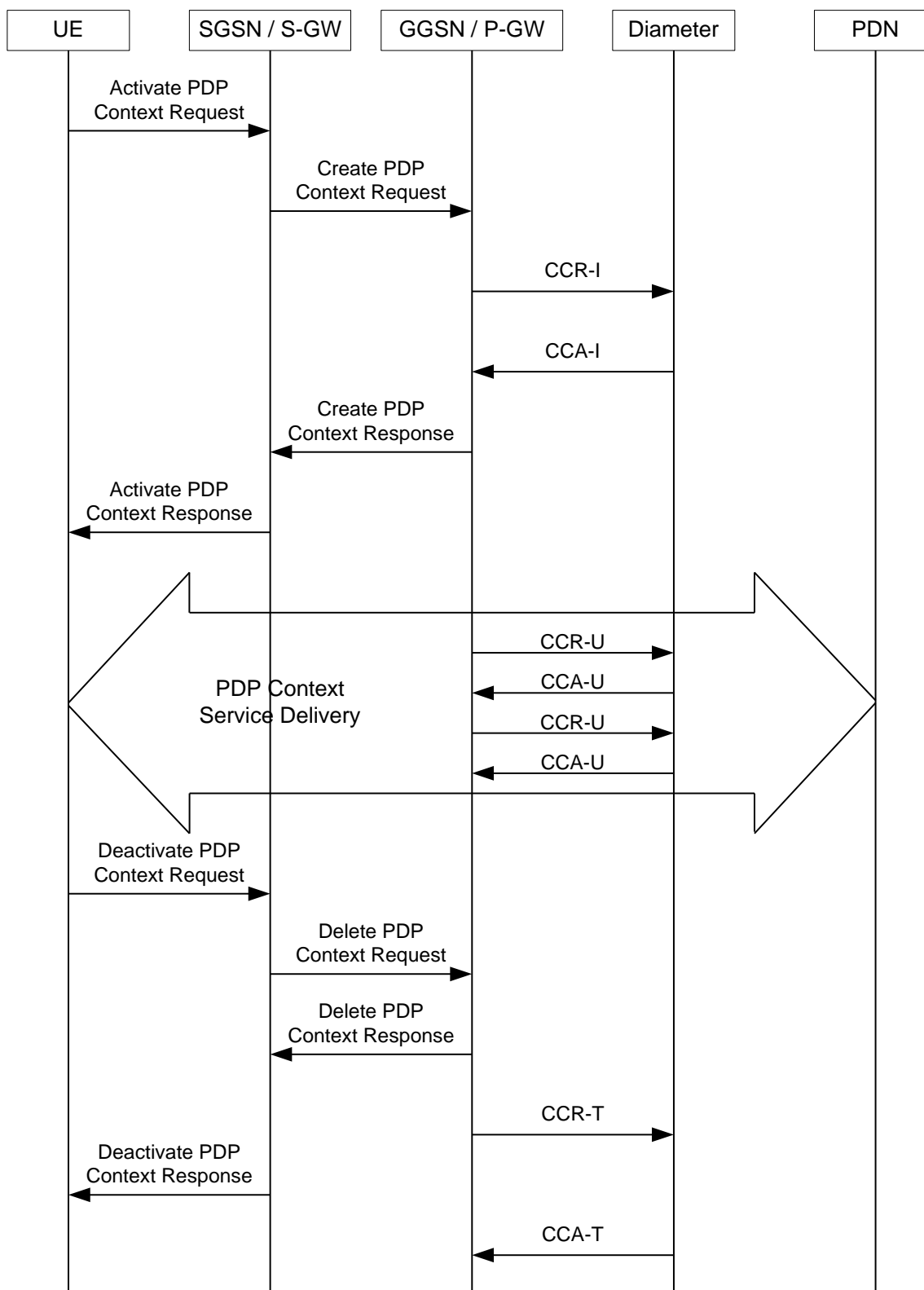
- Credit Control Request - Initial (CCR-I)
- Credit Control Request - Update (CCR-U)
- Credit Control Request - Terminate (CCR-T)
- Credit Control Answer (CCA)
- Credit Control Answer - Initial (CCA-I)
- Credit Control Answer - Update (CCA-U)

If the MSCC AVP is missing in CCA-Update it is treated as invalid CCA and the session is terminated.

- Credit Control Answer - Terminate (CCA-T)

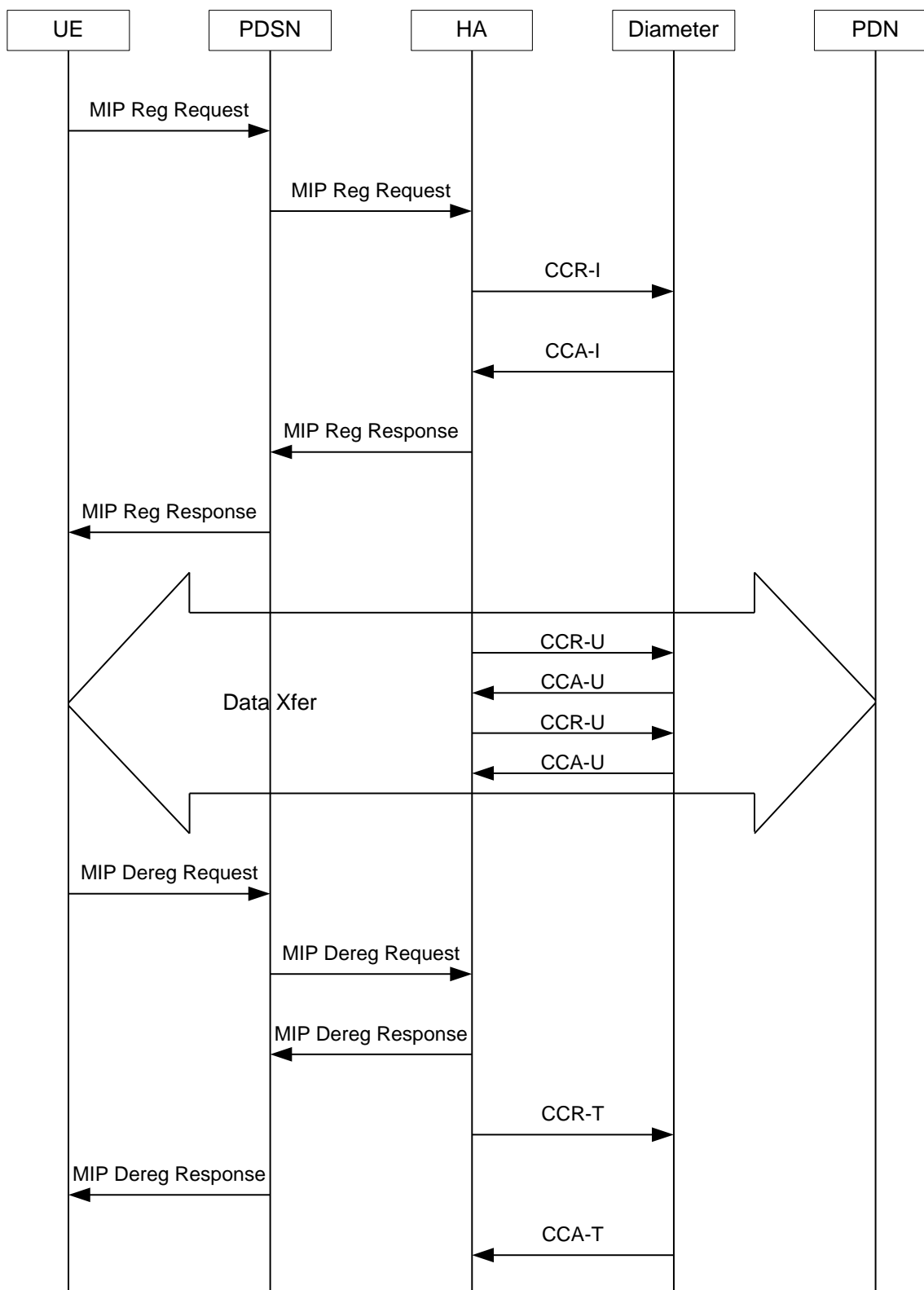
The following figure depicts the call flow for a simple call request in the GGSN / P-GW /IPSG Gy implementation.

Figure 47. Gy Call Flow for Simple Call Request



The following figure depicts the call flow for a simple call request in the HA Gy implementation.

Figure 48. Gy Call Flow for Simple Call Request





## Tx Timer Expiry Behavior

A timer is started each time a CCR is sent out from the system, and the response has to arrive within Tx time. The timeout value is configurable in the Diameter Credit Control Configuration mode.

In case there is no response from the Diameter server for a particular CCR, within Tx time period, and if there is an alternate server configured, the CCR is sent to the alternate server after Tw expiry as described in “Tw Timer expiry behavior” section.

It also depends on the Credit-Control-Session-Failover AVP value for the earlier requests. If this AVP is present and is coded to FAILOVER\_SUPPORTED then the credit-control message stream is moved to the secondary server, in case it is configured. If the AVP value is FAILOVER\_NOT\_SUPPORTED, then the call is dropped in case of failures, even if a secondary server is configured.

## Redirection

In the Final-Unit-Indication AVP, if the Final-Action is REDIRECT or Redirect-Server AVP is present at command level, redirection is performed.

The redirection takes place at the end of consumption of quota of the specified category. The GY sends a CCR-Update without any RSU or Rating-Group AVP so that the server does not give any more quotas.

If the Final-Action AVP is RESTRICT\_ACCESS, then according to the settings in Restriction-Filter-Rule AVP or Filter-Id AVP. GY sends CCR-Update to the server with used quota.

## Triggers

The Diameter server can provide with the triggers for which the client should reauthorize a particular category. The triggers can be configured locally as well but whatever trigger is present in the CCA from the server will have precedence.



**Important:** In this release, Gy triggers are not supported for HA.

The trigger types that are supported are:

- SGSN/Serving-Node Change
- QoS Change - Any
- RAT Change
- LAC Change
- CellID Change

On any event as described in the Trigger type happens, the client reauthorizes quota with the server. The reporting reason is set as RATING\_CONDITION\_CHANGE.

## Tariff Time Change

The tariff change mechanism applies to each category instance active at the time of the tariff change whenever the server indicated it should apply for this category.

The concept of dual coupon is supported. Here the server grants two quotas, which is accompanied by a Tariff-Time-Change, in this case the first granted service unit is used until the tariff change time, once the tariff change time is reached the usage is reported up to the point and any additional usage is not accumulated, and then the second granted service unit is used.

If the server expects a tariff change to occur within the validity time of the quota it is granting, then it includes the Tariff-Time-Change AVP in the CCA. The DCCA report usage, which straddles the change time by sending two instances of the Used-Service-Unit AVP, one with Tariff-Change-Usage set to UNIT\_BEFORE\_TARIFF\_CHANGE, and one with Tariff-Change-Usage set to UNIT\_AFTER\_TARIFF\_CHANGE, and this independently of the type of units used by application. Both Volume and Time quota are reported in this way.

The Tariff time change functionality can as well be done using Validity-Time AVP, where in the Validity-Time is set to Tariff Time change and the client will reauthorize and get quota at Validity-Time expiry. This will trigger a lot of reauthorize request to the server at a particular time and hence is not advised.

Tariff-Time-Usage AVP along with the Tariff-Time-Change AVP in the answer message to the client indicates that the quotas defined in Multiple-Services-Credit-Control are to be used before or after the Tariff Time change. Two separate quotas are allocated one for before Tariff-Time-Change and one for after Tariff-Time-Change. This gives the flexibility to the operators to allocate different quotas to the users for different periods of time. In this case, the DCCA should not send the Before-Usage and After-Usage counts in the update messages to the server. When Tariff-Time-Change AVP is present without Tariff-Time-Usage AVP in the answer message, then the quota is used as in single quota mechanism and the client has to send before usage and after usage quotas in the updates to the server.



**Important:** In this release, Gy does not support UNIT\_INDETERMINATE value.

## Final Unit Indication

The Final-Unit-Indication AVP can be present in the CCA from the server to indicate that the given quota is the final quota from the server and the corresponding action as specified in the AVP needs to be taken.

## Final Unit Indication at Command Level

Gy currently does not support FUI AVP at command level. If this AVP is present at command level it is ignored. If the FUI AVP is present at command level and the Final-Unit-Action AVP set to TERMINATE, Gy sends a CCR-Terminate at the expiry of the quota, with all quotas in the USU AVP.



**Important:** FUI AVP at command level is only supported for Terminate action.

## Final Unit Indication at MSCC Level

If the Final-Unit-Indication AVP is present at MSCC level, and if the Final-Unit-Action AVP is set to TERMINATE, a CCR-Update is sent at the expiry of the allotted quota and report the usage of the category that is terminated.

For information on redirection cases refer to Redirection section.

## Credit Control Failure Handling

CCFH AVP defines what needs to be done in case of failure of any type between the client and the server. The CCFH functionality can be defined in configuration but if the CCFH AVP is present in the CCA, it takes precedence. CCFH AVP gives flexibility to have different failure handling.

Gy supports the following Failure Handling options:

- TERMINATE
- CONTINUE
- RETRY AND TERMINATE

## CCFH with Failover Supported

In case there is a secondary server is configured and if the CC-Session-Failover AVP is set to `FAILOVER_SUPPORTED`, the following behavior takes place:

- **Terminate:** On any Tx expiry for the CCR-I the message is discarded and the session is torn down. In case of CCR-Updates and Terminates the message is sent to the secondary server after response timeout and the session is proceeded with the secondary server. In case there is a failure with the secondary server too, the session is torn down.
- **Continue:** On any Tx expiry, the message is sent to the secondary server after response timeout and the session is proceeded with the secondary server. In case there is a failure with the secondary server too, the session is still established, but without quota management.
- **Retry and Terminate:** On any Tx expiry, the message is sent to the secondary server after the response timeout. In case there is a failure with secondary server too, the session is taken down.

## CCFH with Failover Not Supported

In case there is a secondary server configured and if the CC-Session-Failover AVP is set to `FAILOVER_NOT_SUPPORTED`, the following behavior takes place as listed below. Same is the case if there is no secondary server configured on the system.

- **Terminate:** On any Tx expiry, the session is taken down.
- **Continue:** On any Tx expiry, the session is still established, but without quota management.
- **Retry and Terminate:** On any Tx expiry, the session is taken down.

## Failover Support

The CC-Session-Failover AVP and the Credit-Control-Failure-Handling (CCFH) AVP may be returned by the CC server in the CCA-I, and are used by the DCCA to manage the failover procedure. If they are present in the CCA they override the default values that are locally configured in the system.

If the CC-Session-Failover is set to `FAILOVER_NOT_SUPPORTED`, a CC session will never be moved to an alternative Diameter Server.

If the value of CC-Session-Failover is set to `FAILOVER_SUPPORTED`, then the Gy attempts to move the CC session to the alternative server when it considers a request to have failed, i.e:

- On receipt of result code “`DIAMETER_UNABLE_TO_DELIVER`”, “`DIAMETER_TOO_BUSY`”, or “`DIAMETER_LOOP_DETECTED`”.
- On expiry of the request timeout.
- On expiry of Tw without receipt of DWA, if the server is connected directly to the client.

The CCFH determines the behavior of the client in fault situations. If the Tx timer expires then based on the CCFH value the following actions are taken:

- **CONTINUE:** Allow the MIP session and user traffic for the relevant category or categories to continue, regardless of the interruption (delayed answer). Note that quota management of other categories is not affected.
- **TERMINATE:** Terminate the MIP session, which affects all categories.
- **RETRY\_AND\_TERMINATE:** Allow the MIP session and user traffic for the relevant category or categories to continue, regardless of the interruption (delayed answer). The client retries to send the CCR when it determines a failure-to-send condition and if this also fails, the MIP session is then terminated.

After the failover action has been attempted, and if there is still a failure to send or temporary error, depending on the CCFH action, the following action is taken:

- CONTINUE: Allow the MIP session to continue.
- TERMINATE: Terminate the MIP session.
- RETRY\_AND\_TERMINATE: Terminate the MIP session.

## Recovery Mechanisms

DCCA supports a recovery mechanism that is used to recover sessions without much loss of data in case of Session Manager failures. There is a constant check pointing of Gy data at regular intervals and at important events like update, etc.

For more information on recovery mechanisms, please refer to the *System Administration Guide*.

## Error Mechanisms

### Unsupported AVPs

All unsupported AVPs from the server with “M” bit set are ignored.

### Invalid Answer from Server

If there is an invalid answer from the server, Gy action is dependent on the CCFH setting:

- In case of continue, the MIP session context is continued without further control from Gy.
- In case of terminate and retry-and-terminate, the MIP session is terminated and a CCR-T is sent to the diameter server.

## Result Code Behavior

- DIAMETER\_RATING\_FAILED: On reception of this code, Gy discards all traffic for that category and does not request any more quota from the server. This is supported at the MSCC level and not at the command level.
- DIAMETER\_END\_USER\_SERVICE\_DENIED: On reception of this code, Gy temporarily blacklists the category and further traffic results in requesting new quota from the server. This is supported at the MSCC level and not at the command level.
- DIAMETER\_CREDIT\_LIMIT\_REACHED: On reception of this code, Gy discards all traffic for that category and waits for a configured time, after which if there is traffic for the same category requests quota from the server. This is supported at the MSCC level and not at the command level.
- DIAMETER\_CREDIT\_CONTROL\_NOT\_APPLICABLE: On reception of this code, Gy allows the session to establish, but without quota management. This is supported only at the command level and not at the MSCC level.
- DIAMETER\_USER\_UNKNOWN: On reception of this code, DCCA does not allow the credit control session to get established, the session is terminated. This result code is supported only at the command level and not at the MSCC level.

For all other permanent/transient failures, Gy action is dependent on the CCFH setting.

## Supported AVPs

The Gy functionality supports the following AVPs:

- Supported Diameter Credit Control AVPs specified in RFC 4006:
  - CC-Input-Octets (AVP Code: 412):  
Gy supports this AVP only in USU.
  - CC-Output-Octets (AVP Code: 414):  
Gy supports this AVP only in USU.
  - CC-Request-Number (AVP Code: 415)
  - CC-Request-Type (AVP Code: 416):  
Gy currently does not support EVENT\_REQUEST value.
  - CC-Service-Specific-Units (AVP Code: 417)
  - CC-Session-Failover (AVP Code: 418)
  - CC-Time (AVP Code: 420):  
Gy does not support this AVP in RSU.
  - CC-Total-Octets (AVP Code: 421):  
Gy does not support this AVP in RSU.
  - Credit-Control-Failure-Handling (AVP Code: 427)
  - Final-Unit-Action (AVP Code: 449):  
Supported at Multiple-Services-Credit-Control grouped AVP level and not at command level.
  - Final-Unit-Indication (AVP Code: 430):  
Fully supported at Multiple-Services-Credit-Control grouped AVP level and partially supported (TERMINATE) at command level.
  - Granted-Service-Unit (AVP Code: 431)
  - Multiple-Services-Credit-Control (AVP Code: 456)
  - Multiple-Services-Indicator (AVP Code: 455)
  - Rating-Group (AVP Code: 432)
  - Redirect-Address-Type (AVP Code: 433):  
Gy currently supports only URL (2) value.
  - Redirect-Server (AVP Code: 434)
  - Redirect-Server-Address (AVP Code: 435)
  - Requested-Service-Unit (AVP Code: 437)
  - Result-Code (AVP Code: 268)
  - Service-Context-Id (AVP Code: 461)
  - Service-Identifier (AVP Code: 439)
  - Subscription-Id (AVP Code: 443)
  - Subscription-Id-Data (AVP Code: 444)
  - Subscription-Id-Type (AVP Code: 450)
  - Tariff-Change-Usage (AVP Code: 452):  
Gy does NOT support UNIT\_INDETERMINATE (2) value.

- Tariff-Time-Change (AVP Code: 451)
- Used-Service-Unit (AVP Code: 446):
  - Gy sends only incremental counts for all the AVPs from the last CCA-U.
- User-Equipment-Info (AVP Code: 458)
- User-Equipment-Info-Type (AVP Code: 459):
  - Gy currently supports only IMEISV value.
  - Cisco GGSN and P-GW support IMEISV by default.
- User-Equipment-Info-Value (AVP Code: 460)
- Validity-Time (AVP Code: 448)
- Supported 3GPP specific AVPs specified in 3GPP TS 32.299:
  - 3GPP-Charging-Characteristics (AVP Code: 13)
  - 3GPP-Charging-Id (AVP Code: 2)
  - 3GPP-GGSN-MCC-MNC (AVP Code: 9)
  - 3GPP-GPRS-QoS-Negotiated-Profile (AVP Code: 5)
  - 3GPP-IMSI-MCC-MNC (AVP Code: 8)
  - 3GPP-NSAPI (AVP Code: 10)
  - 3GPP-PDP-Type (AVP Code: 3)
  - 3GPP-RAT-Type (AVP Code: 21)
  - 3GPP-Selection-Mode (AVP Code: 12)
  - 3GPP-Session-Stop-Indicator (AVP Code: 11)
  - 3GPP-SGSN-MCC-MNC (AVP Code: 18)
  - 3GPP-User-Location-Info (AVP Code: 22)
  - Base-Time-Interval (AVP Code: 1265)
  - Charging-Rule-Base-Name (AVP Code: 1004)
  - Envelope (AVP Code: 1266)
  - Envelope-End-Time (AVP Code: 1267)
  - Envelope-Reporting (AVP Code: 1268)
  - Envelope-Start-Time (AVP Code: 1269)
  - GGSN-Address (AVP Code: 847)
  - Offline-Charging (AVP Code: 1278)
  - PDP-Address (AVP Code: 1227)
  - PDP-Context-Type (AVP Code: 1247)
    - This AVP is present only in CCR-I.
  - PS-Information (AVP Code: 874)
  - Quota-Consumption-Time (AVP Code: 881):
    - This optional AVP is present only in CCA.
  - Quota-Holding-Time (AVP Code: 871):

This optional AVP is present only in the CCA command. It is contained in the Multiple-Services-Credit-Control AVP. It applies equally to the granted time quota and to the granted volume quota.

- Reporting-Reason (AVP Code: 872):

Gy currently does not support the POOL\_EXHAUSTED (8) value. It is used in case of credit-pooling which is currently not supported.
- Service-Information (AVP Code: 873):

Only PS-Information is supported.
- SGSN-Address (AVP Code: 1228)
- Time-Quota-Mechanism (AVP Code: 1270):

The Gy server may include this AVP in an Multiple-Services-Credit-Control AVP when granting time quota.
- Time-Quota-Threshold (AVP Code: 868)
- Time-Quota-Type (AVP Code: 1271)
- Trigger (AVP Code: 1264)
- Trigger-Type (AVP Code: 870)
- Unit-Quota-Threshold (AVP Code: 1226)
- Volume-Quota-Threshold (AVP Code: 869)
- Supported Diameter AVPs specified in 3GPP TS 32.299 V8.1.0:
  - Auth-Application-Id (AVP Code: 258)
  - Destination-Host (AVP Code: 293)
  - Destination-Realm (AVP Code: 283)
  - Disconnect-Cause (AVP Code: 273)
  - Error-Message (AVP Code: 281)
  - Event-Timestamp (AVP Code: 55)
  - Failed-AVP (AVP Code: 279)
  - Multiple-Services-Credit-Control (AVP Code: 456)
  - Origin-Host (AVP Code: 264)
  - Origin-Realm (AVP Code: 296)
  - Origin-State-Id (AVP Code: 278)
  - Redirect-Host (AVP Code: 292)
  - Redirect-Host-Usage (AVP Code: 261)
  - Redirect-Max-Cache-Time (AVP Code: 262)
  - Rating-Group (AVP Code: 432)
  - Result-Code (AVP Code: 268)
  - Route-Record (AVP Code: 282)
  - Session-Id (AVP Code: 263)
  - Service-Context-Id (AVP Code: 461)
  - Service-Identifier (AVP Code: 439)

- Supported-Vendor-Id (AVP Code: 265)
- Termination-Cause (AVP Code: 295)
- Used-Service-Unit (AVP Code: 446)
- User-Name (AVP Code: 1)

## Unsupported AVPs

This section lists the AVPs that are NOT supported.

- NOT Supported Credit Control AVPs specified in RFC 4006:
  - CC-Correlation-Id
  - CC-Money
  - CC-Sub-Session-Id
  - CC-Unit-Type (AVP Code: 454)
  - Check-Balance-Result
  - Cost-Information (AVP Code: 423)
  - Cost-Unit (AVP Code: 445)
  - Credit-Control
  - Currency-Code (AVP Code: 425)
  - Direct-Debiting-Failure-Handling (AVP Code: 428)
  - Exponent (AVP Code: 429)
  - G-S-U-Pool-Identifier (AVP Code: 453)
  - G-S-U-Pool-Reference (AVP Code: 457)
  - Requested-Action (AVP Code: 436)
  - Service-Parameter-Info (AVP Code: 440)
  - Service-Parameter-Type (AVP Code: 441)
  - Service-Parameter-Value (AVP Code: 442)
  - Unit-Value (AVP Code: 424)
  - Value-Digits (AVP Code: 447)
- NOT supported Diameter AVPs specified in 3GPP TS 32.299 V8.1.0:
  - Acct-Application-Id (AVP Code: 259)
  - Error-Reporting-Host (AVP Code: 294)
  - Experimental-Result (AVP Code: 297)
  - Experimental-Result-Code (AVP Code: 298)
  - Proxy-Host
  - Proxy-Info
  - Proxy-State
- NOT supported 3GPP-specific AVPs specified in 3GPP TS 32.299 V8.1.0:



- 3GPP-CAMEL-Charging-Info (AVP Code: 24)
- 3GPP-MS-TimeZone (AVP Code: 23)
- 3GPP-PDSN-MCC-MNC
- Authorised-QoS
- Access-Network-Information
- Adaptations
- Additional-Content-Information
- Additional-Type-Information
- Address-Data
- Address-Domain
- Addressee-Type
- Address-Type
- AF-Correlation-Information
- Alternate-Charged-Party-Address
- Application-provided-Called-Party-Address
- Application-Server
- Application-Server-Information
- Applic-ID
- Associated-URI
- Aux-Applic-Info
- Bearer-Service
- Called-Asserted-Identity
- Called-Party-Address
- Calling-Party-Address
- Cause-Code
- Charged-Party
- Class-Identifier
- Content-Class
- Content-Disposition
- Content-Length
- Content-Size
- Content-Type
- Data-Coding-Scheme
- Deferred-Location-Event-Type

- Delivery-Report-Requested
- Destination-Interface
- Domain-Name
- DRM-Content
- Early-Media-Description
- Event
- Event-Type
- Expires
- File-Repair-Supported
- IM-Information
- IMS-Charging-Identifier (ICID)
- IMS-Communication-Service-Identifier
- IMS-Information
- Incoming-Trunk-Group-ID
- Interface-Id
- Interface-Port
- Interface-Text
- Interface-Type
- Inter-Operator-Identifier
- LCS-APN
- LCS-Client-Dialed-By-MS
- LCS-Client-External-ID
- LCS-Client-ID
- LCS-Client-Name
- LCS-Client-Type
- LCS-Data-Coding-Scheme
- LCS-Format-Indicator
- LCS-Information
- LCS-Name-String
- LCS-Requestor-ID
- LCS-Requestor-ID-String
- Location-Estimate
- Location-Estimate-Type
- Location-Type

- Low-Balance-Indication
- MBMS-Information
- MBMS-User-Service-Type
- Media-Initiator-Flag
- Media-Initiator-Party
- Message-Body
- Message-Class
- Message-ID
- Message-Size
- Message-Type
- MMBox-Storage-Requested
- MM-Content-Type
- MMS-Information
- Node-Functionality
- Number-Of-Participants
- Number-Of-Received-Talk-Bursts
- Number-Of-Talk-Bursts
- Originating-IOI
- Originator
- Originator-Address
- Originator-Interface
- Originator-SCCP-Address
- Outgoing-Trunk-Group-ID
- Participant-Access-Priority
- Participants-Group
- Participants-Involved
- PDG-Address
- PDG-Charging-Id
- PoC-Change-Condition
- PoC-Change-Time
- PoC-Controlling-Address
- PoC-Group-Name
- PoC-Information
- PoC-Server-Role

- PoC-Session-Id
- PoC-Session-Initiation-Type
- PoC-Session-Type
- PoC-User-Role
- PoC-User-Role-IDs
- PoC-User-Role-info-Units
- Positioning-Data
- Priority
- PS-Append-Free-Format-Data (AVP Code: 867):

The PCEF/GW ignores this AVP if no PS free format data is stored for the online charging session.

- PS-Free-Format-Data (AVP Code: 866)
- PS-Furnish-Charging-Information (AVP Code: 865)
- RAI (AVP Code: 909)
- Read-Reply-Report-Requested
- Received-Talk-Burst-Time
- Received-Talk-Burst-Volume
- Recipient-Address
- Recipient-SCCP-Address
- Refund-Information
- Remaining-Balance
- Reply-Applic-ID
- Reply-Path-Requested
- Requested-Party-Address
- Role-of-node
- SDP-Answer-Timestamp
- SDP-Media-Component
- SDP-Media-Description
- SDP-Media-Name
- SDP-Offer-Timestamp
- SDP-Session-Description
- SDP-TimeStamp
- Served-Party-IP-Address
- Service-Generic-Information
- Service-ID
- Service-Specific-Data

- Service-Specific-Info
- Service-Specific-Type
- SIP-Method
- SIP-Request-Timestamp
- SIP-Response-Timestamp
- SM-Discharge-Time
- SM-Message-Type
- SM-Protocol-Id
- SMSC-Address
- SMS-Information
- SMS-Node
- SM-Status
- SM-User-Data-Header
- Submission-Time
- Talk-Burst-Exchange
- Talk-Burst-Time
- Talk-Burst-Volume
- Terminating-IOI
- Time-Stamps
- Token-Text
- Trunk-Group-ID
- Type-Number
- User-Participating-Type
- User-Session-ID
- WAG-Address
- WAG-PLMN-Id
- WLAN-Information
- WLAN-Radio-Container
- WLAN-Session-Id
- WLAN-Technology
- WLAN-UE-Local-IPAddress

## Configuring Gy Interface Support

To configure Gy interface support:

1. Configure the core network service as described in this Administration Guide.
2. Configure Gy interface support as described in the relevant section:
  - [Configuring GGSN / P-GW / IPSG Gy Interface Support](#)
  - [Configuring HA / PDSN Gy Interface Support](#)
3. Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.



**Important:** Commands used in the configuration examples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the *Command Line Interface Reference* for complete information regarding all commands.

## Configuring GGSN / P-GW / IPSG Gy Interface Support

To configure the standard Gy interface support for GGSN/P-GW/IPSG, use the following configuration:

**configure**

```
context <context_name>

    diameter endpoint <endpoint_name>

        origin realm <realm>

        origin host <diameter_host> address <ip_address>

        peer <peer> realm <realm> address <ip_address>

    exit

exit

active-charging service <ecs_service_name>

    credit-control [ group <cc_group_name> ]

        diameter origin endpoint <endpoint_name>

        diameter peer-select peer <peer> realm <realm>

        diameter pending-timeout <timeout_period>

        diameter session failover
```

```

    diameter dictionary <dictionary>

    failure-handling initial-request continue

    failure-handling update-request continue

    failure-handling terminate-request continue

    exit

exit

context <context_name>

    apn <apn_name>

        selection-mode sent-by-ms

        ims-auth-service <service>

        ip access-group <access_list_name> in

        ip access-group <access_list_name> out

        ip context-name <context_name>

        active-charging rulebase <rulebase_name>

        credit-control-group <cc_group_name>

    end

```

#### Notes:

- For information on configuring IP access lists, refer to the *Access Control Lists* chapter in the *System Administration Guide*.
- For more information on configuring ECS ruledefs, refer to the *ACS Ruledef Configuration Mode Commands* chapter in the *Command Line Interface Reference*.
- For more information on configuring ECS charging actions, refer to the *ACS Charging Action Configuration Mode Commands* chapter in the *Command Line Interface Reference*.
- For more information on configuring ECS rulebases, refer to the *ACS Rulebase Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

## Configuring HA / PDSN Gy Interface Support

To configure HA / PDSN Gy interface support, use the following configuration:

```

configure

    context <context_name>

        diameter endpoint <endpoint_name>

```

```

    origin realm <realm>

    origin host <diameter_host> address <ip_address>

    peer <peer> realm <realm> address <ip_address>

    exit

exit

active-charging service <ecs_service_name>

    ruledef <ruledef_name>

        ip any-match = TRUE

        exit

    charging-action <charging_action_name>

        content-id <content_id>

        cca charging credit rating-group <rating_group>

        exit

    rulebase <rulebase_name>

        action priority <action_priority> ruledef <ruledef_name> charging-action
<charging_action_name>

        exit

    credit-control [ group <cc_group_name> ]

        diameter origin endpoint <endpoint_name>

        diameter peer-select peer <peer> realm <realm>

        diameter pending-timeout <timeout>

        diameter session failover

        diameter dictionary <dictionary>

        failure-handling initial-request continue

        failure-handling update-request continue

        failure-handling terminate-request continue

        pending-traffic-treatment noquota buffer

        pending-traffic-treatment quota-exhausted buffer

        exit

```



```

exit

context <context_name>

  subscriber default

    ip access-group <acl_name> in

    ip access-group <acl_name> out

    ip context-name <context_name>

    active-charging rulebase <rulebase_name>

    credit-control-group <cc_group_name>

  end

```

#### Notes:

- For information on configuring IP access lists, refer to the *Access Control Lists* chapter in the *Systems Administration Guide*.
- For more information on configuring ECS ruledefs, refer to the *ACS Ruledef Configuration Mode Commands* chapter in the *Command Line Interface Reference*.
- For more information on configuring ECS charging actions, refer to the *ACS Charging Action Configuration Mode Commands* chapter in the *Command Line Interface Reference*.
- For more information on configuring ECS rulebases, refer to the *ACS Rulebase Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

## Gathering Statistics

This section explains how to gather Gy and related statistics and configuration information.

In the following table, the first column lists what statistics to gather, and the second column lists the action to perform.

Statistics/Information	Action to perform
Complete statistics for ECS sessions.	<b>show active-charging sessions full</b>
Information on all rule definitions configured in the service.	<b>show active-charging ruledef all</b>
Information on all charging actions configured in the service.	<b>show active-charging charging-action all</b>
Information on all rulebases configured in the service.	<b>show active-charging rulebase all</b>
Statistics of the Credit Control application, DCCA.	<b>show active-charging credit-control statistics</b>
States of the Credit Control application's sessions, DCCA.	<b>show active-charging credit-control session-states [ rulebase &lt;rulebase_name&gt; ] [ content-id &lt;content_id&gt; ]</b>



# Appendix E

## ICAP Interface Support

---

This chapter provides information on configuring the external Active Content Filtering servers for a core network service subscriber. This chapter also describes the configuration and commands that are used to implement this feature.

It is recommended that you select the configuration example that best meets your service model, and configure the required elements for that model, as described in respective product Administration Guide, before using the procedures in this chapter.

The following products currently support ICAP interface functionality:

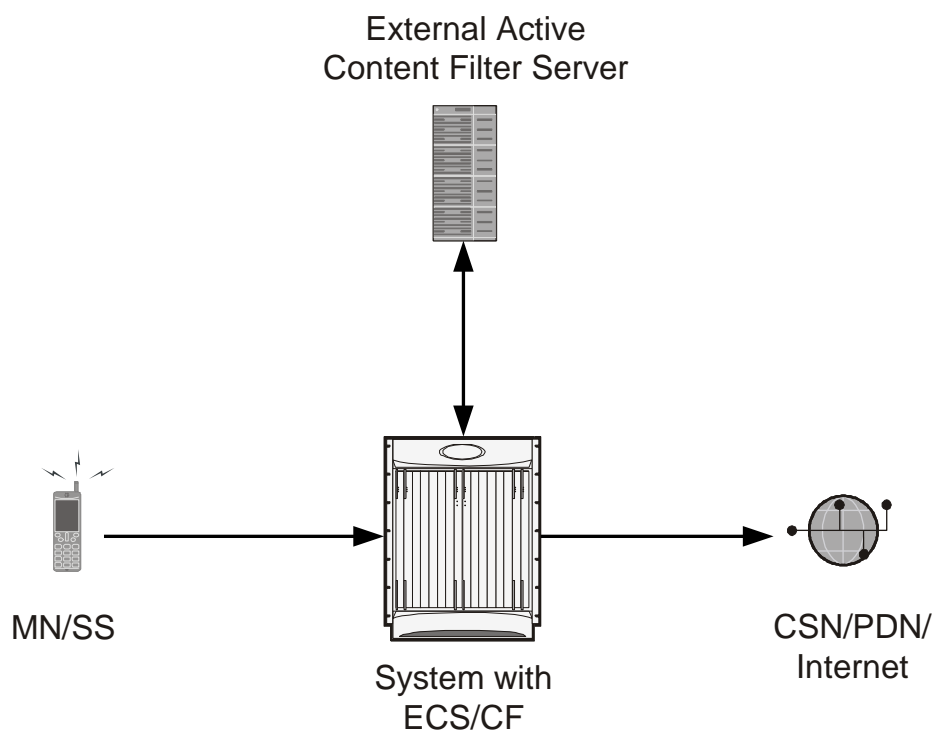
- GGSN
- P-GW

# ICAP Interface Support Overview

This feature supports streamlined ICAP interface to leverage Deep Packet Inspection (DPI) to enable external application servers to provide their services without performing DPI, and without being inserted in the data flow. For example with an external Active Content Filtering (ACF) Platform.

A high-level view of the streamlined ICAP interface support for external ACF is shown in the following figure:

**Figure 49. High-Level View of Streamlined ICAP Interface with external ACF**



The system with ECS is configured to support DPI and the system uses this capability for content charging as well.

If a subscriber initiates a WAP (WAP1.x or WAP2.0) or Web session, the subsequent GET/POST request is detected by the DPI function. The URL of the GET/POST request is extracted and passed, along with subscriber identification information and the subscriber request, in an ICAP message to the application server. The application server checks the URL on the basis of its category and other classifications like, type, access level, content category and decides if the request should be authorized, blocked, or redirected by answering to the GET/POST with:

- A 200 OK message if the request is accepted
- A 302 Redirect message in case of redirection. This redirect message includes the URL to which the subscriber should be redirected
- A 403 Denied message if the request should be blocked

Depending on the response received, the system with ECS will either pass the request unmodified, or discard the message and respond to the subscriber with the appropriate redirection or block message.

Content charging is performed by the Active Charging Service (ACS) only after the request has been controlled by the application server. This guarantees the appropriate interworking between the external application and content-based billing. In particular, this guarantees that charging will be applied to the appropriate request in case of redirection, and that potential charging-based redirections (i.e. Advice of Charge, Top Up page, etc.) will not interfere with the decisions taken by the application server.

Functions of the ACF include:

- Retrieval of subscriber policies based on the subscriber identity passed in the ICAP message
- Determining the appropriate action (permit, deny, redirect) to take for the type of content based on subscriber profile
- Communication of the action (permit, deny, or redirect) decision for the URL back to the ACS module

## Failure Action on Retransmitted Packets

ICAP rating is enabled for retransmitted packet when default ICAP failure action was taken on an ICAP request for that flow. ICAP default failure action is taken on the pending ICAP request for a connection when the connection needs to be reset and there is no other redundant connection available. For example, in the ICAP request timeout and ICAP connection timeout scenarios. In these cases the retransmitted packet in the uplink direction is sent for ICAP rating again.

In case of WAP CO, uplink retransmitted packet for the WAP transactions for which ICAP failure action was taken will be sent for ICAP rating. WSP header of the retransmitted packet is not parsed by the WSP analyzer. The URL received in the previous packet for that transaction is used for ICAP rating. If failure action was taken on multiple WTP transactions for the same flow (case: WTP concatenated GET request) then uplink retransmitted packet for each of the transaction is sent for rating again.

In case of HTTP, uplink retransmitted packets for the HTTP flow on which ICAP failure action is taken is sent for ICAP rating. The URL present in the current secondary session (last uplink request) is used for ICAP rating. However, if there were multiple outstanding ICAP request for the same flow (pipelined request) then for the retransmitted packet the URL that will be sent for rating will be that of the last GET request.

Retransmission in various cases of failure-action taken on re-transmitted packets when the ICAP response is not received for the original request and the retransmitted request comes in:

- WSP CO:
  - Permit: The uplink packet is sent for ICAP rating and depending on the ICAP response the WTP transaction is allowed/blocked. It is possible that the WAP gateway sends the response for the permitted GET request. Hence, there is a race condition and the subscriber may be able to view the web page even though the rating was redirect or content insert.
  - Content Insert: The retransmitted packet is not sent for ICAP rating.
  - Redirect: The retransmitted packet is not sent for ICAP rating.
  - Discard: The uplink packet is sent for ICAP rating and depending on the ICAP response the WTP transaction is allowed/blocked.
  - Terminate flow: The uplink packet is sent for ICAP rating and depending on the ICAP response the WTP transaction is allowed or blocked. The WAP gateway may send an Abort transaction for this GET request if the WSP disconnect packet sent while terminating the flow is received by the WAP gateway.
- HTTP:
  - Permit: The uplink packet is sent for ICAP rating and depending on the ICAP response the last HTTP GET request. It is possible that the HTTP server sends the response for the permitted GET request.

Hence there is a race condition and the subscriber may be able to view the web page even though the rating was redirect or content insert.

- Content Insert: Retransmitted packets are dropped and not charged.
- Redirect: Retransmitted packets are dropped and not charged.
- Discard: The uplink packet is sent for ICAP rating and depending on the ICAP response the WTP transaction allowed/blocked.
- Terminate flow: Retransmitted packets are dropped and not charged.

## Supported Networks and Platforms

This feature supports ST16 and Cisco Chassis for the core network services configured on the system.

## License Requirements


External Content Filtering Server support through Internet Content Adaptation Protocol (ICAP) interface is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements.

For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

## Configuring ICAP Interface Support

This section describes how to configure the Content Filtering Server Group (CFSG) through Internet Content Adaptation Protocol (ICAP) interface between ICAP client and ACF server (ICAP server).

---

 **Important:** This section provides the minimum instruction set for configuring external content filtering servers on ICAP interface on the system. For more information on commands that configure additional parameters and options, refer to *CFSG Configuration Mode Commands* chapter in *Command Line Interface Reference*.

---

To configure the system to provide ICAP interface support for external content filtering servers:

- Step 1** Create the Content Filtering Server Group and create ICAP interface with origin (local) IP address of chassis by applying the example configuration in the [Creating ICAP Server Group and Address Binding](#) section.
- Step 2** Specify the active content filtering server (ICAP sever) IP addresses and configure other parameters for ICAP server group by applying the example configuration in the [Configuring ICAP Server and Other Parameters](#) section.
- Step 3** Configure the content filtering mode to external content filtering server group mode in ECS rule base by applying the example configuration in the [Configuring ECS Rulebase for ICAP Server Group](#) section.
- Step 4** *Optional.* Configure the charging action to forward HTTP/WAP GET request to external content filtering servers on ICAP interface in Active Charging Configuration mode by applying the example configuration in the [Configuring Charging Action for ICAP Server Group](#) section.
- Step 5** Verify your ICAP interface and external content filtering server group configuration by following the steps in the [Verifying the ICAP Server Group Configuration](#) section.
- Step 6** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

## Creating ICAP Server Group and Address Binding

Use the following example to create the ICAP server group and bind the IP addresses:

**configure**

```
context <icap_ctxt_name> [ -noconfirm ]

    content-filtering server-group <icap_svr_grp_name> [ -noconfirm ]

        origin address <ip_address>

    end
```

Notes:

- <ip\_address> is local IP address of the CFSG endpoint.

## Configuring ICAP Server and Other Parameters

Use the following example to configure the active content filtering (ICAP server) and other related parameters:

```
configure

context <icap_context_name>

    content-filtering server-group <icap_server_grp_name>

        icap server <ip_address> [port <port_number>] [max <max_msgs>] [priority
<priority>]

        deny-message <msg_string>

        response-timeout <timeout>

        connection retry-timeout <retry_timeout>

        failure-action {allow | content-insertion <content_string> | discard | redirect-
url <url> | terminate-flow}

        dictionary {custom1 | custom2 | standard}

    end
```

Notes:

- In StarOS 8.1 and later, a maximum of five ICAP servers can be configured per Content Filtering Server Group. In StarOS 8.0, only one ICAP Server can be configured per Content Filtering Server Group.
- The maximum outstanding request per ICAP connection configured using the optional **max** <max\_msgs> keyword is limited to one. Therefore, any other value configured using the **max** keyword will be ignored.
- *Optional.* To configure the ICAP URL extraction behavior, in the Content Filtering Server Group configuration mode, enter the following command:

```
url-extraction { after-parsing | raw }
```

By default, percent-encoded hex characters in URLs sent from the ACF client to the ICAP server will be converted to corresponding ASCII characters and sent.

## Configuring ECS Rulebase for ICAP Server Group

Use the following example to configure the content filtering mode to ICAP server mode in the ECS rulebase for content filtering:

```
configure

require active-charging [optimized-mode]

active-charging service <acs_svc_name> [-noconfirm]

rulebase <rulebase_name> [-noconfirm]

    content-filtering mode server-group <cf_server_group>
```



```
end
```

Notes:

- In StarOS 8.1, the **optimized-mode** keyword enables ACS in the Optimized mode, wherein ACS functionality is managed by SessMgrs. In StarOS 8.1, ACS must be enabled in the Optimized mode.
- In StarOS 8.3, the **optimized-mode** keyword is obsolete. With or without this keyword ACS is always enabled in Optimized mode.
- In StarOS 8.0 and StarOS 9.0 and later, the **optimized-mode** keyword is not available.

## Configuring Charging Action for ICAP Server Group

Use the following example to configure the charging action to forward HTTP/WAP GET request to ICAP server for content processing:

```
configure
```

```
active-charging service <acs_svc_name>

charging-action <charging_action_name> [ -noconfirm ]

content-filtering processing server-group

end
```

## Verifying the ICAP Server Group Configuration

This section explains how to display and review the configurations after saving them in a .cfg file and also to retrieve errors and warnings within an active configuration for a service.



**Important:** All commands listed here are under Exec mode. Not all commands are available on all platforms.

These instructions are used to verify the configuration for this feature.

**Step 1** Verify your ICAP Content Filtering Server Group configuration by entering the following command in Exec Mode:

```
show content-filtering server-group
```

The following is a sample output. In this example, an ICAP Content Filtering server group named *icap\_cfsg1* was configured.

```
Content Filtering Group:    icap_cfsg1

Context:                   icap1

Origin Address:            1.2.3.4

ICAP Address (Port) :      1.2.3.4 (1344)

Max Outstanding:           256
```

```
Priority: 1

Response Timeout: 30(secs)      Connection Retry
Timeout: 30(secs)

Dictionary: standard

Timeout Action: terminate-flow

Deny Message: "Service Not Subscribed"

URL-extraction: after-parsing

Content Filtering Group Connections: NONE

Total content filtering groups matching specified criteria: 1
```

**Step 2** Verify any configuration error in your configuration by entering the following command in Exec Mode:

```
show configuration errors
```

# Appendix F

## IP Pool Sharing Protocol

---

This chapter provides information on configuring an enhanced, or extended, service. The product administration guides provide examples and procedures for configuration of basic services on the system. It is recommended that you select the configuration example that best meets your service model, and configure the required elements for that model before using the procedures in this chapter.

Sections in this chapter include:

- [Overview](#)
- [How IPSP Works](#)
- [Configuring IPSP Before the Software Upgrade](#)
- [Configuring IPSP After the Software Upgrade](#)
- [Disabling IPSP](#)

## Overview

The IP Pool Sharing Protocol (IPSP) is a protocol that system-based HA services can use during an offline-software upgrade to avoid the assignment of duplicate IP addresses to sessions while allowing them to maintain the same address, and to preserve network capacity.

In order for IPSP to be used, at least two system-based HAs with identical configurations must be present on the same LAN. IPSP uses a primary & secondary model to manage the IP pools between the HAs. When used, this protocol ensures the following:

- In-progress sessions can be handed-off to the secondary HA when an offline-software upgrade is being performed on the primary and receive the same IP address that it was originally assigned.
- New sessions can be redirected to the secondary HA when an offline-software upgrade is being performed on the primary and receive a non-duplicate IP address.

The protocol is enabled at the interface level. Each system-based HA must have an IPSP-enabled interface configured in the same context as the HA service for this protocol to function properly.

## Primary HA Functionality

The primary HA is the system that is to be upgraded. It performs the following functions for IPSP:

- Queries the pool information from the secondary HA; the pool configurations on both HAs must be identical
- Assigns an IP address or address block to the secondary HA when requested by the secondary HA; the primary HA releases sessions if they have an IP address requested by the secondary
- For graceful termination conditions (e.g. an administrative user issues the **reload** command), sends a termination message to the secondary HA causing it to assume the responsibilities of the primary HA until the primary is available again.
- Sends a trap when the number of calls drops to zero after starting IPSP

## Secondary HA Functionality

The secondary HA is the system that takes over Mobile IP sessions from the primary HA that is being upgraded. It performs the following functions for IPSP:

- Locks the IP pools until it receives an address or address block assignment from the primary HA; it unlocks the IP pools after busying out the addresses that are not assigned to it
- Processes address requests for sessions that are within the address block assigned to it
- Communicates with the primary HA, as needed, to request IP addresses that are not currently assigned to it; it does not assign the address until the primary HA approves it
- For graceful termination conditions (e.g. an administrative user issues the **reload** command), it notifies the primary HA that it is going out of service
- Assumes the responsibility of the primary HA when requested to
- In the event that it determines that primary HA is not available, it assumes the responsibility of the primary HA if there is at least one address allocated to verify that the AAA server is re-configured to direct the calls

## Requirements, Limitations, & Behavior

- One IPSP interface can be configured per system context.
- The IPSP interfaces for both the primary and secondary HAs must be configured to communicate on the same network.
- If IP pool busyout is enabled on any configured address pool, IPSP can not be configured.
- The IP pool configuration (pool name, addresses, priority, pool group, etc.) on both the HAs must be identical.
- IP pools cannot be modified on either the primary or the secondary HAs once IPSP is enabled.
- Sessions are dropped during the IPSP setup process if:
  - the primary HA has not yet approved an IP address or address block.
  - the primary HA is not known to the secondary HA.
- Once an address is assigned to the secondary HA, all the information about that address is erased on the primary HA and that address becomes unusable by the primary HA.
- LRU is not supported across the systems. Although, LRU continues to be supported within the system.
- If the IPSP configuration is not disabled before removing the HA from the IPSP network link, sessions may be rejected if the system's VPN Manager is rebooted or restarts.
- IPSP does not control static IP pools. An external application (AAA, etc.) must be responsible for ensuring that duplicate addresses are not assigned.
- IPSP ignores interface failures allowing the configured dead-interval timer to determine when the HA should become the primary and control the pool addresses. Before the dead-interval timer starts, the secondary HA maintains its state and any busied out addresses remain busied out. After the dead-interval timer starts, IPSP marks the neighboring peer HA as down, becomes primary, and will unbusy out all pool addresses.

## How IPSP Works

IPSP operation requires special configuration in both the primary and secondary HAs. As mentioned previously, both HAs must have identical configurations. This allows the secondary HA to process sessions identically to the primary when the primary is taken offline for upgrade.

Configuration must also be performed on the AAA server. Whereas subscriber profiles on the AAA server originally directed sessions to the primary HA, prior to using IPSP, subscriber profiles must be re-configured to direct sessions to the secondary HA.

There are two scenarios in which IPSP takes effect:

- **New sessions:** Once IPSP is configured, new sessions are directed to a secondary HA (HA2) allowing the primary HA to go through a software upgrade without degrading network capacity. The secondary HA requests addresses from the primary HA's (HA1) pools as needed. As the addresses are allocated, they are busied out on the primary HA. This procedure is displayed below.
- **Session handoffs:** Once IPSP is configured, sessions originally registered with the primary HA (HA1) are re-registered with the secondary HA (HA2). To ensure the session is assigned the same IP address, the secondary HA requests the address from the primary HA. The primary HA verifies the binding and releases it to the secondary HA which, in turn, re-assigns it to the session. As the addresses are allocated, they are busied out on the primary HA. This procedure is displayed below.

## IPSP Operation for New Sessions

The following figure and text describe how new sessions are handled when IPSP is enabled.

Figure 50. IPSP Operation for New Sessions

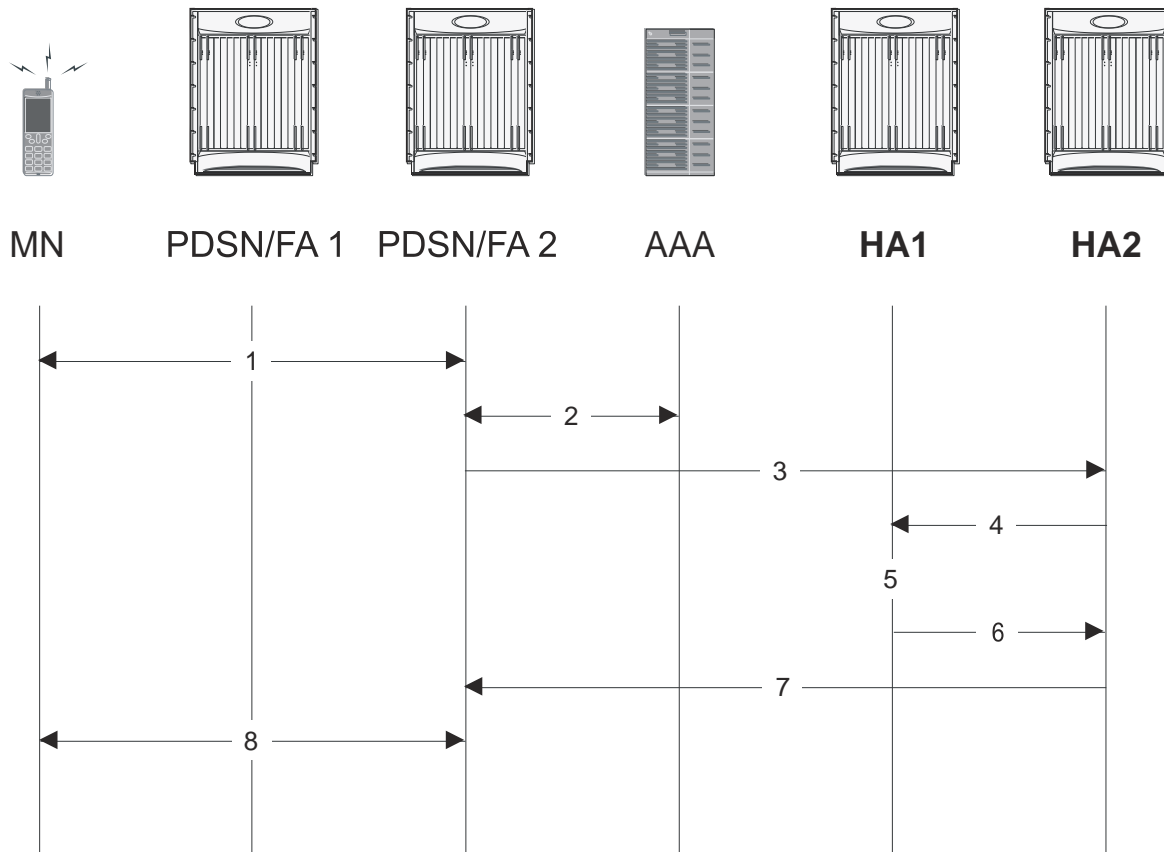


Table 21. IPSP Operation for New Sessions Description

Step	Description
1	A mobile node (MN) attempting to establish a data session is connected to PDSN/FA 2.
2	PDSNFA 2 authenticates the subscriber with the AAA server. One of the attributes returned by the AAA server as part of a successful authentication is the IP address of the secondary HA.
3	PDSN/FA 2 forwards the session request to HA2 for processing. HA2 processes the session as it would for any Mobile IP session.
4	With IPSP enabled, prior to assigning an IP address, HA2 sends a request to HA1 for an IP address.
5	HA1 allocates the address to HA2 and busies it out so it cannot be re-assigned.
6	HA1 responds to HA2 with the IP address for the session.
7	HA2 proceeds with session processing and provides PDSN/FA 2 with the IP address for the MN.
8	The MN and PDSN/FA 2 complete session processing.

## IPSP Operation for Session Handoffs

The following figure and text describe how session handoffs are handled when IPSP is enabled.

Figure 51. IPSP Operation for Session Handoffs

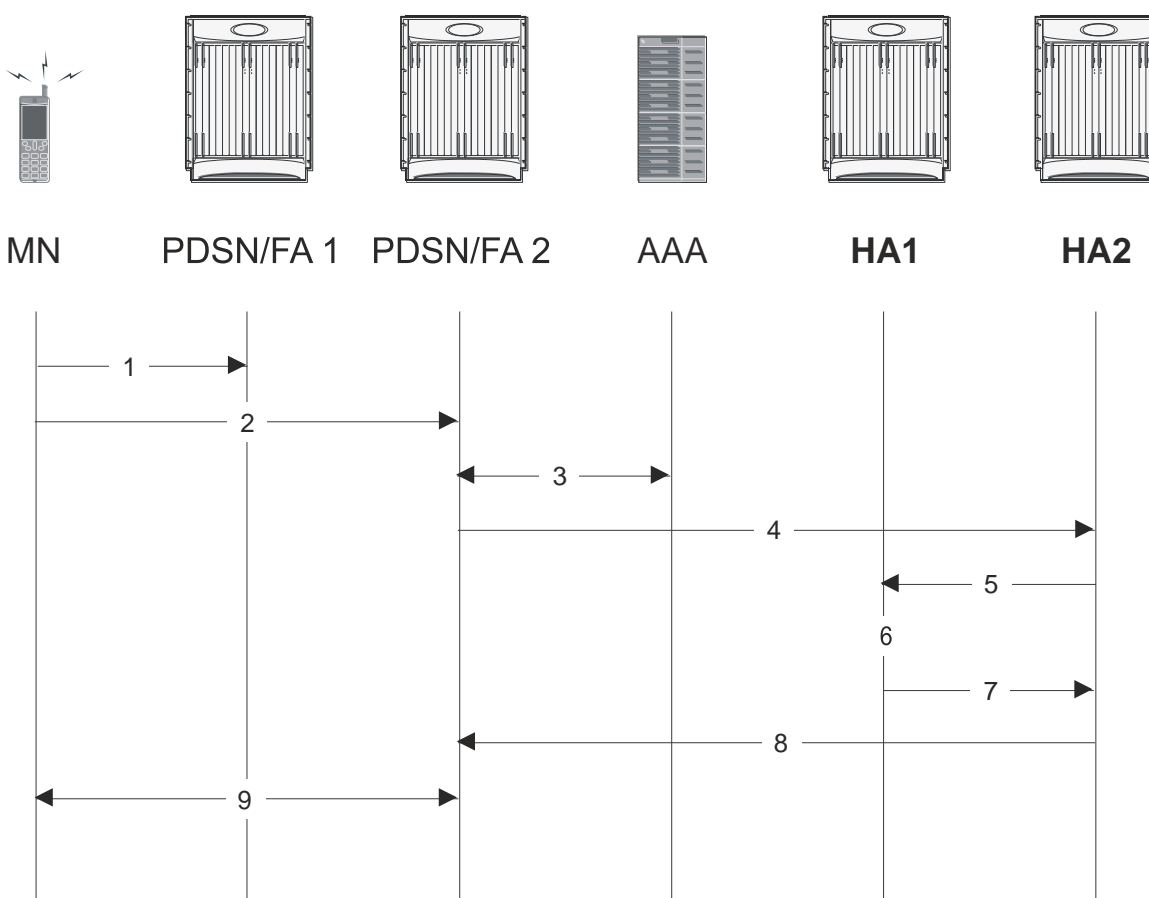


Table 22. IPSP Operation for Session Handoffs Description

Step	Description
1	A mobile node (MN) is connected to PDSN/FA 1.
2	The MN's session is handed-off to PDSN/FA2 and goes through the re-registration process.
3	PDSN/FA 2 authenticates the subscriber with the AAA server as part of the re-registration process. One of the attributes returned by the AAA server as part of a successful authentication is the IP address of the secondary HA.
4	PDSN/FA 2 forwards the session request to HA2 for processing. Included in the request is the MN's current IP address.
5	With IPSP enabled, prior to assigning an IP address, HA2 sends a request to HA1 for an IP address.
6	HA1 verifies the MN's information and releases the binding. It then busies out the address so it cannot be re-assigned.
7	HA1 allocates the original IP address to HA2 for the session.



Step	Description
8	HA2 proceeds with session processing and provides PDSN/FA 2 with the IP address for the mobile node.
9	The mobile node and PDSN/FA 2 complete session processing.

## Configuring IPSP Before the Software Upgrade

Configuring IPSP requires changes to the primary HA (the HA on which the software upgrade is to occur), the secondary HA (the HA to which subscribers sessions are to be directed), and the AAA server.

This section provides information and instructions for configuring IPSP before the software upgrade.



**Important:** This section provides the minimum instruction set for configuring IPSP on the system. For more information on commands that configure additional parameters and options, refer to the *IPSP Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

To enable the IP pool sharing during software upgrade:

- Step 1** Configure the AAA servers by applying the example configuration in the [Configuring the AAA Server for IPSP](#) section.
- Step 2** Configure an interface on the system for use by IPSP according to the instructions found in the *Creating and Configuring Ethernet Interfaces and Ports* section of the *System Administration Guide*.
- Step 3** Enable the IPSP on secondary HA by applying the example configuration in the [Enabling IPSP on the Secondary HA](#) section.
- Step 4** Perform the boot system priority and SPC/SMC card synchronization as described in *Off-line Software Upgrade* section in the *System Administration Guide*.
- Step 5** Enable the IPSP on primary HA by applying the example configuration in the [Enabling IPSP on the Primary HA](#) section.
- Step 6** Verify your ACL configuration by following the steps in the *Verifying the IPSP Configuration* section.
- Step 7** Proceed for software upgrade as described in *Off-line Software Upgrade* section in the *System Administration Guide*.
- Step 8** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

## Configuring the AAA Server for IPSP

For subscriber session establishment, the AAA server provides the IP address of the HA that is to service the session. This information exists in the 3GPP2\_MIP\_HA\_Address RADIUS attribute configured for the subscriber.

Because the primary HA has been responsible for facilitating subscriber sessions, its IP address is the one configured via this attribute. For IPSP however, the attribute configuration must change in order to direct sessions to the secondary HA.


To do this, reconfigure the 3GPP2\_MIP\_HA\_Address RADIUS attribute for each subscriber on the AAA server with the IP address of the secondary HA.

The precise instructions for performing this operation vary depending on the AAA server vendor. Refer to the documentation for your AAA server for more information.

## Enabling IPSP on the Secondary HA

The secondary HA is the alternate HA that is to take responsibility while the primary HA is upgraded.

---

 **Important:** This section provides the minimum instruction set for configuring IPSP on the system. For more information on commands that configure additional parameters and options, refer to the *IPSP Configuration Mode Commands* chapter in *Command Line Interface Reference*.

---

Use the following example to enable the IPSP on secondary HA:

```
configure

context <ipsp_ctxt_name> [ -noconfirm ]

    interface <ipsp_if_name>

        pool-share-protocol primary <pri_ha_address> [ mode {active | inactive |
check-config } ]

        dead-interval <dur_sec>

    end
```


Notes:

- The interface must be configured in the same context as the HA service and must be on the same network as the primary HA's IPSP interface.
- *ipsp\_if\_name* is the name of the interface on which you want to enable IPSP.
- *dead-interval* is an optional command to configure time to wait before retrying the primary HA for the IP Pool Sharing Protocol.

## Enabling IPSP on the Primary HA

The primary HA is the HA that is to be upgraded.

---

 **Important:** This section provides the minimum instruction set for configuring IPSP on the system. For more information on commands that configure additional parameters and options, refer to the *IPSP Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

---

Use the following example to enable the IPSP on primary HA:

```
configure

context <ipsp_ctxt_name> [ -noconfirm ]

    interface <ipsp_if_name>

        pool-share-protocol secondary <sec_ha_address> [ mode {active | inactive
| check-config } ]
```

```
dead-interval <dur_sec>

end
```

Notes:

- The interface must be configured in the same context as the HA service and must be on the same network as the secondary HA's IPSP interface.
- *ipsp\_if\_name* is the name of the interface on which you want to enable IPSP.
- *dead-interval* is an optional command to configure time to wait before retrying the secondary HA for the IP Pool Sharing Protocol.



**Important:** Once this configuration is done, the primary HA begins to hand responsibility for sessions and release IP addresses to the secondary HA. Prior to performing the software upgrade, all IP addresses must be released. When IPSP has released all IP pool addresses from the primary HA an SNMP trap (**starIPSPAllAddrsFree**) is triggered.

## Verifying the IPSP Configuration

These instructions are used to verify the IPSP configuration.

Verify that IPSP has released all IP addresses by entering the following command in Exec Mode with in specific context:


```
show ip ipsp
```

The output of this command provides the list of used addresses and released addresses. The system will send the **starIPSPAllAddrsFree** trap once all IP addresses are released. When the value in the *Used Addresses* column reaches 0 for all IP pools listed, then the primary HA sends the SNMP trap and notifies the secondary HA to take over as the primary HA.

## Configuring IPSP After the Software Upgrade

If desired, IP pool addresses can be migrated from the original secondary HA back to the original primary HA once the upgrade process is complete.

---


 **Important:** It is important to note that the HA that was originally designated as the secondary is now functioning as the primary HA. Conversely, the HA that was originally designated as the primary is now functioning as the secondary.

---

In order to migrate the addresses, both HAs and the AAA server must be configured according to the instructions in this section.

This section provides information and instructions for configuring IPSP after the software upgrade.

---

 **Important:** This section provides the minimum instruction set for configuring IPSP on the system. For more information on commands that configure additional parameters and options, refer *IPSP Configuration Mode Commands* chapter in *Command Line Interface Reference*.

---

To enable the IP pool sharing after software upgrade:

- Step 1** Configure the AAA servers by applying the example configuration in the [Configuring the AAA Server for IPSP](#) section.
- Step 2** Configure an interface on the system for use by IPSP according to the instructions found in the Creating and Configuring Ethernet Interfaces and Ports section of *System Administration Guide*.
- Step 3** Enable the IPSP on secondary HA by applying the example configuration in the [Enabling IPSP on the Secondary HA](#) section.
- Step 4** Enable the IPSP on primary HA by applying the example configuration in the [Enabling IPSP on the Primary HA](#) section.
- Step 5** Verify your ACL configuration by following the steps in the *Verifying the IPSP Configuration* section.
- Step 6** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

## Disabling IPSP

Once all IP addresses on the primary HA have been released, IPSP must be disabled on both the primary and secondary HAs.



**Caution:** Prior to disabling IPSP, ensure that the primary HA has released all IP addresses to secondary HA.

---

Follow the instructions in this section to disable IPSP on primary and secondary HA after migration of all IP addresses.



**Important:** This section provides the minimum instruction set for disabling IPSP on the HAs. For more information on commands, refer to the *IPSP Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

---

Use the following example to enable the IPSP on primary/secondary HA:

```
configure

context <ipsp_ctxt_name> [ -noconfirm ]

    interface <ipsp_if_name>

        no pool-share-protocol

    end
```

Notes:

- The interface must be configured in the same context as the primary/secondary HA service and must be on the same network as the primary/secondary HA's IPSP interface.
- *ipsp\_if\_name* is the name of the interface on which you want to disable IPSP.
- IPSP must be disabled on both the HAs.

# Appendix G

## IP Header Compression

---

This chapter provides information on configuring an enhanced, or extended, service. The product administration guides provide examples and procedures for configuration of basic services on the system. It is recommended that you select the configuration example that best meets your service model, and configure the required elements for that model, as described in the respective product administration guide, before using the procedures in this chapter.



**Important:** RoHC header compression is not applicable for SGSN and GGSN services.

---

This chapter includes the following procedures:

- [Configuring VJ Header Compression for PPP](#)
- [Configuring RoHC Header Compression for PPP](#)
- [Configuring Both RoHC and VJ Header Compression](#)
- [Configuring RoHC for Use with SO67 in PDSN or HSGW Service](#)
- [Using an RoHC Profile for Subscriber Sessions](#)
- [Disabling VJ Header Compression Over PPP](#)
- [Disabling RoHC Header Compression Over SO67](#)
- [Checking IP Header Compression Statistics](#)
- [RADIUS Attributes for IP Header Compression](#)

## Overview

The system supports IP header compression on the PPP tunnels established over the EVDO-RevA A10 links and also over the GRE tunnel that is connected to the PCF to support EVDO-RevA Service Option 67 (SO67).

By default IP header compression using the VJ algorithm is enabled for subscribers using PPP.

Note that you can use the default VJ header compression algorithm alone, configure the use of RoHC header compression only, or use both VJ and RoHC IP header compression.

- **Van Jacobsen (VJ)** - The RFC 1144 (CTCP) header compression standard was developed by V. Jacobson in 1990. It is commonly known as VJ compression. It describes a basic method for compressing the headers of IPv4/TCP packets to improve performance over low speed serial links.
- **RObust Header Compression (RoHC)** - The RFC 3095 (RoHC) standard was developed in 2001. This standard can compress IP/UDP/RTP headers to just over one byte, even in the presence of severe channel impairments. This compression scheme can also compress IP/UDP and IP/ESP packet flows. RoHC is intended for use in wireless radio network equipment and mobile terminals to decrease header overhead, reduce packet loss, improve interactive response, and increase security over low-speed, noisy wireless links.



**Important:** The RoHC is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

In addition, you can configure RoHC profiles that define RoHC Compressor and Decompressor parameters. These RoHC profiles can be applied to subscribers.

You can also turn off all IP header compression for a subscriber.

The procedures in this chapter describe how to configure the IP header compression methods used, but for RoHC over PPP the Internet Protocol Control Protocol (IPCP) negotiations determine when they are used.

Implementing IP header compression provides the following benefits:

- Improves interactive response time
- Allows the use of small packets for bulk data with good line efficiency
- Allows the use of small packets for delay sensitive low data-rate traffic
- Decreases header overhead.
- Reduces packet loss rate over lossy links.




## Configuring VJ Header Compression for PPP

By default, VJ IP header compression is enabled for subscriber sessions. When VJ header compression is configured all IP headers are compressed using the VJ compression algorithm.

Note that procedure described in this section is applicable only when VJ header compression is disabled.

---

 **Important:** This section provides the minimum instruction set for configuring subscriber profile for header compression. For more information on commands that configure additional parameters and options, refer *Subscriber Configuration Mode Commands* chapter in *Command Line Interface Reference* .

---

To configure the system to enable VJ header compression to IP headers:

- Step 1** Enable VJ header compression by applying the example configuration in the [Enabling VJ Header Compression](#) section.
- Step 2** Verify your VJ header compression configuration by following the steps in the [Verifying the VJ Header Compression Configuration](#) section.
- Step 3** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

## Enabling VJ Header Compression

Use the following example to enable the VJ header compression over PPP:

```
configure

context <ctxt_name>

    subscriber name <subs_name>

        ip header-compression vj

    end
```

Notes:

- *<ctxt\_name>* is the system context in which you wish to configure the subscriber profile. Typically this is an AAA context.
- *<subs\_name>* is the name of the subscriber in the current context that you want to enable VJ IP header compression for.

## Verifying the VJ Header Compression Configuration

These instructions are used to verify the VJ header compression configuration.

- Step 1** Verify that your header compression configurations for subscriber by entering the following command in Exec Mode in specific context:


```
show subscriber configuration username subs_name
```

The output of this command is a concise listing of subscriber parameter settings as configured.

## Configuring RoHC Header Compression for PPP

RoHC IP header compression can be configured for all IP traffic, uplink traffic only, or downlink traffic only. When RoHC is configured for all traffic, you can specify the mode in which RoHC is applied.

---

 **Important:** This section provides the minimum instruction set for configuring subscriber profile for header compression. For more information on commands that configure additional parameters and options, refer *Subscriber Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

---

To configure the system to enable RoHC header compression to IP headers:

- Enable RoHC header compression by applying the example configuration in the [Enabling RoHC Header Compression for PPP](#) section.
- Verify your RoHC header compression configuration by following the steps in the [Verifying the Header Compression Configuration](#) section.
- Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

## Enabling RoHC Header Compression for PPP

Use the following example to enable the RoHC over PPP:

```
configure

context <ctxt_name>

    subscriber name <subs_name>

        ip header-compression RoHC [ any [ mode { optimistic | reliable | unidirectional
} ] | cid-mode { { large | small } [ marked-flows-only | max-cid | max-hdr <value> | mrru
<value> ] } | marked flows-only | max-hdr <value> | mrru <value> | downlink | uplink ] ]+

    end
```

Notes:

- <ctxt\_name> is the system context in which you wish to configure the subscriber profile. Typically this is an AAA context.
- <subs\_name> is the name of the subscriber in the current context that you want to enable RoHC header compression for.
- Refer to the *Subscriber Configuration Mode Commands* chapter in *Command Line Interface Reference* for more details on this command and its options.

## Verifying the Header Compression Configuration

These instructions are used to verify the header compression configuration.


- Step 1** Verify that your header compression configurations for subscriber by entering the following command in Exec Mode in specific context:


```
show subscriber configuration username subs_name
```

The output of this command is a concise listing of subscriber parameter settings as configured.

## Configuring Both RoHC and VJ Header Compression

You can configure the system to use both VJ and RoHC IP header compression. When both VJ and RoHC are specified, the optimum header compression algorithm for the type of data being transferred is used for data in the downlink direction.

 **Important:** If both RoHC and VJ header compression are specified, the optimum header compression algorithm for the type of data being transferred is used for data in the downlink direction.

 **Important:** This section provides the minimum instruction set for configuring subscriber profile for header compression. For more information on commands that configure additional parameters and options, refer *Subscriber Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

To configure the system to enable both RoHC and VJ header compression to IP headers:

- Enable the RoHC and VJ header compression by applying the example configuration in the [Enabling RoHC and VJ Header Compression for PPP](#) section.
- Verify your RoHC and VJ header compression configuration by following the steps in the [Verifying the Header Compression Configuration](#) section.
- Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

## Enabling RoHC and VJ Header Compression for PPP

Use the following example to enable the header compression over PPP:

```
configure

context <ctxt_name>

    subscriber name <subs_name>

        ip header-compression vj RoHC [ any [ mode { optimistic | reliable |
unidirectional } ] | cid-mode { { large | small } [ marked-flows-only | max-cid | max-hdr
<value> | mrru <value> ] } | marked flows-only | max-hdr <value> | mrru <value> |
downlink | uplink ] ]+

    end
```

Notes:

- *<ctxt\_name>* is the system context in which you wish to configure the subscriber profile. Typically this is an AAA context.
- *<subs\_name>* is the name of the subscriber in the current context that you want to enable RoHC header compression for.

- Refer to the Subscriber Configuration Mode Commands chapter in Command Line Interface Reference for more details on this command and its options.

## Verifying the Header Compression Configuration

These instructions are used to verify the header compression configuration.


- Step 1** Verify that your header compression configurations for subscriber by entering the following command in Exec Mode in specific context:

```
show subscriber configuration username subs_name
```

The output of this command is a concise listing of subscriber parameter settings as configured.

## Configuring RoHC for Use with SO67 in PDSN or HSGW Service

This section explains how to set RoHC settings in the PDSN or HSGW Service configuration mode. These settings are transferred to the PCF during the initial A11 setup and are used for the GRE tunnel that is connected to the PCF to support EVDO-RevA Service Option 67 (SO67). RoHC is enabled through an auxiliary SO67 A10 connection and the PCF signals this information when the auxiliary A10 is connected.

 **Important:** This section provides the minimum instruction set for configuring subscriber profile for header compression. For more information on commands that configure additional parameters and options, refer *PDSN Service Configuration Mode Commands* or *HSGW Service Configuration Mode Commands* chapter in *Command Line Interface Reference*.

To configure the system to enable the RoHC header compression feature at the PDSN or HSGW Service over SO67:

- Step 1** Enable header compression by applying the example configuration in the [Enabling ROHC Header Compression with PDSN](#) or [Enabling ROHC Header Compression with HSGW](#) section.
- Step 2** Verify your RoHC configuration by following the steps in the [Verifying the Header Compression Configuration](#) section.
- Step 3** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

### Enabling RoHC Header Compression with PDSN

Use the following example to enable the RoHC header compression with PDSN over SO67:

```
configure

context <ctxt_name>

    pdsn-service <svc_name>

        ip header-compression rohc

        cid-mode {large | small} max-cid integer

        mrru <num_octets>

        profile { [esp-ip] [rtp-udp] [udp-ip] [uncompressed-ip] }          end
```

Notes:

- *<ctxt\_name>* is the system context in which PDSN service is configured and you wish to configure the service profile.
- *<svc\_name>* is the name of the PDSN service in which you want to enable RoHC over SO67.
- Refer to the *PDSN Service RoHC Configuration Mode Commands* chapter in *Command Line Interface Reference* for more details on this command and its options.

## Enabling RoHC Header Compression with HSGW

Use the following example to enable the RoHC header compression with HSGW over SO67:

```
configure

context <ctxt_name>

    hsgw-service <svc_name>

        ip header-compression rohc

            cid-mode {large | small} max-cid integer

            mrru <num_octets>

            profile { [esp-ip] [rtp-udp] [udp-ip] [uncompressed-ip] }

        end
```

Notes:

- <ctxt\_name> is the system context in which HSGW service is configured and you wish to configure the service profile.
- <svc\_name> is the name of the HSGW service in which you want to enable RoHC over SO67.
- Refer to the *HSGW Service RoHC Configuration Mode Commands* chapter in *Command Line Interface Reference* for more details on this command and its options.

## Verifying the Header Compression Configuration

These instructions are used to verify the header compression configuration.

**Step 1** Verify that your header compression configurations for subscriber by entering the following command in Exec Mode in specific context:

```
show configuration context ctxt_name
```

The output of this command is a concise listing of subscriber parameter settings as configured.



## Using an RoHC Profile for Subscriber Sessions

You can configure RoHC profiles that specify numerous compressor and decompressor settings. These profiles can in turn be applied to a specific subscriber or the default subscriber. RoHC profiles are used for both RoHC over PPP and for RoHC over SO67.



**Important:** This section provides the minimum instruction set for configuring subscriber profile for header compression. For more information on commands that configure additional parameters and options, refer *Subscriber Configuration Mode Commands* chapter in *Command Line Interface Reference*.

To configure the system to apply RoHC profile to a subscriber session:

- Step 1** Create RoHC profile using decompression mode or decompression mode. If you want to use compression mode go to step a else follow step b:
  - Step a.....**Configure RoHC profile by applying the example configuration in the [Creating ROHC Profile for Subscriber using Compression Mode](#) section using compression mode.
  - Step b .....**Alternatively configure RoHC profile by applying the example configuration in the [Creating ROHC Profile for Subscriber using Decompression Mode](#) section using compression mode.
- Step 2** Apply existing RoHC profile to a subscriber by applying the example configuration in the [Applying ROHC Profile to a Subscriber](#) section.
- Step 3** Verify your RoHC header compression configuration by following the steps in the [Verifying the Header Compression Configuration](#) section.
- Step 4** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

## Creating RoHC Profile for Subscriber using Compression Mode

Use the following example to create RoHC profile for a subscriber using compression mode:

```
configure

RoHC-profile profile-name <RoHC_comp_profile_name>

  decompression-options

    [no] multiple-ts-stride

    rtp-sn-p <p_value>

    [no] use-ipid-override

    [no] use-optimized-talkspurt

    [no] use-optimized-transience
```

```
[no] use-timer-based-compression

end
```

Notes:

- `<RoHC_comp_profile_name>` is the name of the RoHC profile with compression mode which you want to apply to a subscriber.
- System configured most of the parameters by default. For more information on other options and parameters and details, refer to the *RoHC Profile Compression Configuration Mode Commands* chapter in *Command Line Interface Reference*.

## Creating RoHC Profile for Subscriber using Decompression Mode

Use the following example to create RoHC profile for a subscriber using decompression mode:

```
configure
```

```
RoHC-profile profile-name <RoHC_decomp_profile_name>

  decompression-options

    context-timeout <dur>

    max-jitter-cd <dur_ms>

    nak-limit <limit>

    optimistic-mode-ack

    optimistic-mode-ack-limit <num_pkts>

    piggyback-wait-time <dur_ms>

    preferred-feedback-mode { bidirectional-optimistic | bidirectional-reliable |
unidirectional }

    rtp-sn-p <p_value>

    [no] rtp-sn-p-override

    [no] use-clock-option

    [no] use-crc-option

    [no] use-feedback

    [no] use-jitter-option

    [no] use-reject-option

    [no] use-sn-option

  end
```

Notes:

- `<RoHC_profile_name>` is the name of the RoHC profile with decompression mode which you want to apply to a subscriber.
- System configured most of the parameters by default. For more information on other options and parameters and details, refer to the *RoHC Profile Decompression Configuration Mode Commands* chapter in *Command Line Interface Reference*.

## Applying RoHC Profile to a Subscriber

Once an RoHC profile has been created that profile can be specified to be used for a specific subscribers. Use the following example to apply the RoHC profile to a subscriber:

```
configure

context <ctxt_name>

    subscriber name <subs_name>

        RoHC-profile-name <RoHC_profile_name>

    end
```

Notes:

- `<ctxt_name>` is the system context in which you wish to configure the subscriber profile. Typically this is an AAA context.
- `<subs_name>` is the name of the subscriber in the current context that you want to enable RoHC header compression for.
- `<RoHC_profile_name>` is the name of the existing RoHC profile (created with compressed or decompressed mode) which you want to apply to a subscriber in the current context.
- Refer to the *Subscriber Configuration Mode Commands* chapter in *Command Line Interface Reference* for more details on this command and its options.

## Verifying the Header Compression Configuration

These instructions are used to verify the header compression configuration.

**Step 1** Verify that your header compression configurations for subscriber by entering the following command in Exec Mode in specific context:

```
show subscriber configuration username subs_name
```

The output of this command is a concise listing of subscriber parameter settings as configured.

## Disabling VJ Header Compression Over PPP

By default, VJ IP header compression is enabled for subscriber sessions. When VJ header compression is configured all IP headers are compressed using the VJ compression algorithm.

If you do not want to apply compression to any IP headers for a subscriber session you can disable the IP header compression feature.



**Important:** This section provides the minimum instruction set for configuring subscriber profile for header compression. For more information on commands that configure additional parameters and options, refer *Subscriber Configuration Mode Commands* chapter in *Command Line Interface Reference*.

To configure the system to disable VJ header compression to IP headers:

- Step 1** Disable header compression by applying the example configuration in the [Disabling VJ Header Compression](#) section.
- Step 2** Verify your VJ header compression configuration by following the steps in the [Verifying the VJ Header Compression Configuration](#) section.
- Step 3** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

## Disabling VJ Header Compression

Use the following example to disable the VJ header compression over PPP:

```
configure

context <ctxt_name>

    subscriber name <subs_name>

    no ip header-compression

end
```

Notes:

- <ctxt\_name> is the system context in which you wish to configure the subscriber profile. Typically this is an AAA context.
- <subs\_name> is the name of the subscriber in the current context that you want to disable IP header compression for.

## Verifying the VJ Header Compression Configuration

These instructions are used to verify the VJ header compression configuration.

**Step 1** Verify that your header compression configurations for subscriber by entering the following command in Exec Mode in specific context:

```
show subscriber configuration username <subs_name>
```

The output of this command is a concise listing of subscriber parameter settings as configured.

## Disabling RoHC Header Compression Over SO67

If you do not want to apply compression to any IP headers for a subscriber sessions using the EVDO-RevA SO67 feature, you can disable the IP header compression feature at the PDSN or HSGW Service.



**Important:** This section provides the minimum instruction set for configuring subscriber profile for header compression. For more information on commands that configure additional parameters and options, refer *PDSN Service Configuration Mode Commands* or *HSGW Service Configuration Mode Commands* chapter in *Command Line Interface Reference*.

To configure the system to disable the IP header compression feature at the PDSN or HSGW Service:

- Step 1** Disable header compression by applying the example configuration in the [Disabling ROHC Header Compression](#) section.
- Step 2** Verify your RoHC configuration by following the steps in the [Verifying the Header Compression Configuration](#) section.
- Step 3** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

## Disabling RoHC Header Compression

Use the following example to disable the header compression over SO67:

```
configure

context <ctxt_name>

    pdsn/hsgw-service <svc_name>

        no ip header-compression RoHC

    end
```

Notes:

- <ctxt\_name> is the system context in which PDSN or HSGW service is configured and you wish to configure the service profile.
- <svc\_name> is the name of the PDSN or HSGW service in which you want to disable RoHC over SO67.

## Verifying the Header Compression Configuration

These instructions are used to verify the header compression configuration.

- Step 1** Verify that your header compression configurations for subscriber by entering the following command in Exec Mode in specific context:

```
show configuration context <ctxt_name>
```

The output of this command is a concise listing of subscriber parameter settings as configured.

## Checking IP Header Compression Statistics

This section contains commands to use to retrieve statistics that include IP header compression information.

The following Exec mode commands can be used to retrieve IP header compression statistics:

- `monitor protocol ppp`
- `show ppp`
- `show ppp statistics`
- `show RoHC statistics`
- `show RoHC statistics pdsn-service`
- `show subscriber full username`

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



## RADIUS Attributes for IP Header Compression

This section lists the names of the RADIUS attributes to use for RoHC header compression. For more information on these attributes, refer to the AAA Interface Administration and Reference.

One of the following attributes can be used to specify the name of the RoHC profile to use for the subscriber session:

- SN-RoHC-Profile-Name
- SN1-RoHC-Profile-Name

Any RoHC parameters not specified in the RoHC profile are set to their default values.




# Appendix H

## IP Security


---

This chapter provides information on configuring an enhanced or extended service. The product Administration Guides provide examples and procedures for configuration of basic services on the system. It is recommended that you select the configuration example that best meets your service model, and configure the required elements for that model, as described in the respective product Administration Guide, before using the procedures in this chapter.

---

 **Important:** The IP Security is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

---

 **Caution:** IPSec parameter configurations saved using this release may not function properly with older software releases.

---

This chapter contains the following sections:

- [Overview](#)
- [IPSec Terminology](#)
- [Implementing IPSec for PDN Access Applications](#)
- [Implementing IPSec for Mobile IP Applications](#)
- [Implementing IPSec for L2TP Applications](#)
- [Transform Set Configuration](#)
- [ISAKMP Policy Configuration](#)
- [ISAKMP Crypto Map Configuration](#)
- [Dynamic Crypto Map Configuration](#)
- [Manual Crypto Map Configuration](#)
- [Crypto Map and Interface Association](#)
- [FA Services Configuration to Support IPSec](#)
- [HA Service Configuration to Support IPSec](#)
- [RADIUS Attributes for IPSec-based Mobile IP Applications](#)
- [LAC Service Configuration to Support IPSec](#)
- [Subscriber Attributes for L2TP Application IPSec Support](#)
- [PDSN Service Configuration for L2TP Support](#)
- [Redundant IPSec Tunnel Fail-Over](#)
- [Redundant IPSec Tunnel Fail-over Configuration](#)
- [Dead Peer Detection \(DPD\) Configuration](#)

## ■ RADIUS Attributes for IP Header Compression

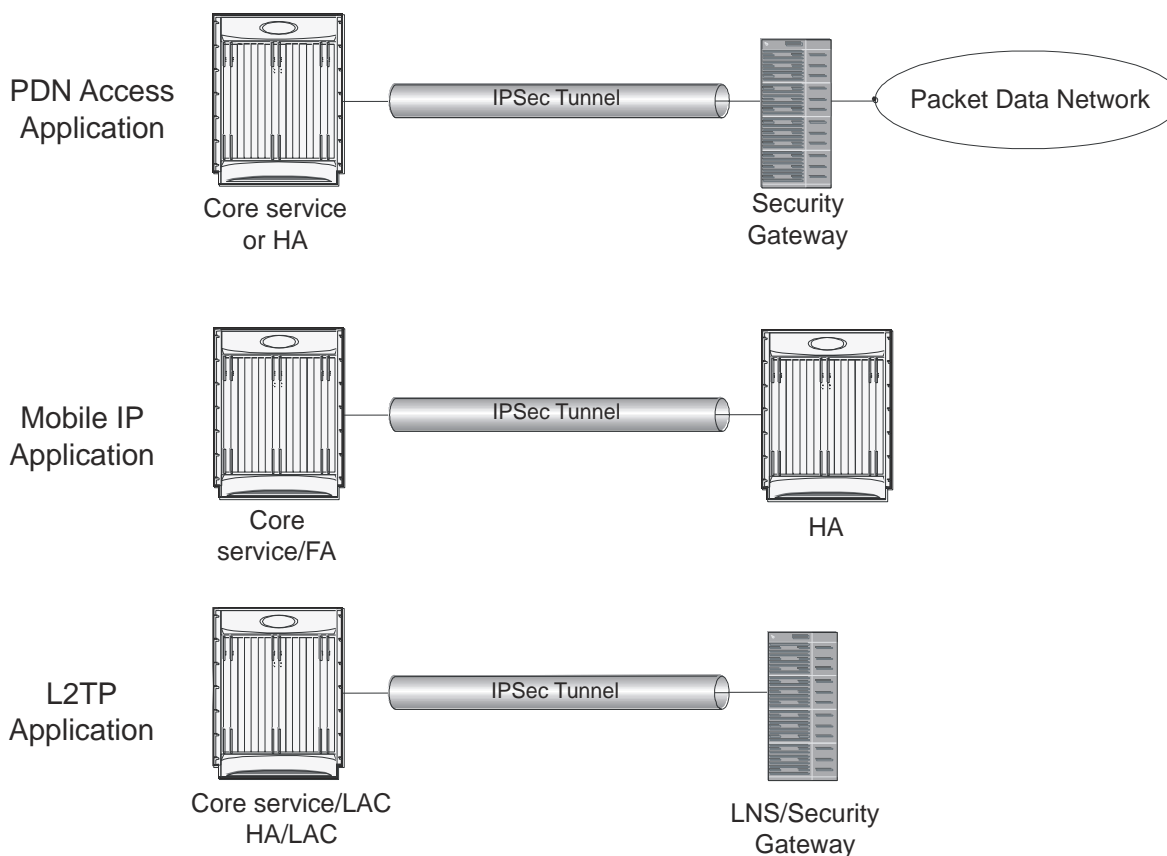
- [APN Template Configuration to Support L2TP](#)
- [IPSec for LTE/SAE Networks](#)

## Overview

IP Security (IPSec) is a suite of protocols that interact with one another to provide secure private communications across IP networks. These protocols allow the system to establish and maintain secure tunnels with peer security gateways. IPSec can be implemented on the system for the following applications:

- **PDN Access:** Subscriber IP traffic is routed over an IPSec tunnel from the system to a secure gateway on the packet data network (PDN) as determined by access control list (ACL) criteria. This application can be implemented for both core network service and HA-based systems. The following figure shows IPSec configurations.

Figure 52. IPSec Applications



- **Mobile IP:** Mobile IP control signals and subscriber data is encapsulated in IPSec tunnels that are established between foreign agents (FAs) and home agents (HAs) over the Pi interfaces.



**Important:** Once an IPSec tunnel is established between an FA and HA for a particular subscriber, all new Mobile IP sessions using the same FA and HA are passed over the tunnel regardless of whether or not IPSec is supported for the new subscriber sessions. Data for existing Mobile IP sessions is unaffected.

- **L2TP:** L2TP-encapsulated packets are routed from the system to an LNS/secure gateway over an IPSec tunnel.

Note that: IPSec can be implemented for both attribute-based and compulsory tunneling applications for 3GPP2 services.

## Applicable Products and Relevant Sections

The IPSec feature is supported for various products. The following table indicates the products on which the feature is supported and the relevant sections within the chapter that pertain to that product.

Applicable Product(s)	Refer to Sections
PDSN/FA/HA	<ul style="list-style-type: none"> <li>• <a href="#">Implementing IPSec for PDN Access Applications</a></li> <li>• <a href="#">Implementing IPSec for Mobile IP Applications</a></li> <li>• <a href="#">Transform Set Configuration</a></li> <li>• <a href="#">ISAKMP Policy Configuration</a></li> <li>• <a href="#">ISAKMP Crypto Map Configuration</a></li> <li>• <a href="#">Dynamic Crypto Map Configuration</a></li> <li>• <a href="#">Manual Crypto Map Configuration</a></li> <li>• <a href="#">Crypto Map and Interface Association</a></li> <li>• <a href="#">FA Services Configuration to Support IPSec</a></li> <li>• <a href="#">HA Service Configuration to Support IPSec</a></li> <li>• <a href="#">RADIUS Attributes for IPSec-based Mobile IP Applications</a></li> <li>• <a href="#">LAC Service Configuration to Support IPSec</a></li> <li>• <a href="#">Subscriber Attributes for L2TP Application IPSec Support</a></li> <li>• <a href="#">PDSN Service Configuration for L2TP Support</a></li> <li>• <a href="#">Redundant IPSec Tunnel Fail-Over</a></li> <li>• <a href="#">Dead Peer Detection (DPD) Configuration</a></li> </ul>

Applicable Product(s)	Refer to Sections
GGSN/FA/HA	<ul style="list-style-type: none"><li>• <a href="#">Implementing IPsec for PDN Access Applications</a></li><li>• <a href="#">Implementing IPsec for Mobile IP Applications</a></li><li>• <a href="#">Implementing IPsec for L2TP Applications</a></li><li>• <a href="#">Transform Set Configuration</a></li><li>• <a href="#">ISAKMP Policy Configuration</a></li><li>• <a href="#">ISAKMP Crypto Map Configuration</a></li><li>• <a href="#">Dynamic Crypto Map Configuration</a></li><li>• <a href="#">Manual Crypto Map Configuration</a></li><li>• <a href="#">Crypto Map and Interface Association</a></li><li>• <a href="#">FA Services Configuration to Support IPsec</a></li><li>• <a href="#">HA Service Configuration to Support IPsec</a></li><li>• <a href="#">RADIUS Attributes for IPsec-based Mobile IP Applications</a></li><li>• <a href="#">LAC Service Configuration to Support IPsec</a></li><li>• <a href="#">Redundant IPsec Tunnel Fail-Over</a></li><li>• <a href="#">Dead Peer Detection (DPD) Configuration</a></li><li>• <a href="#">TAPN Template Configuration to Support L2TP</a></li></ul>

Applicable Product(s)	Refer to Sections
ASN GW	<ul style="list-style-type: none"><li>• <a href="#">Implementing IPsec for PDN Access Applications</a></li><li>• <a href="#">Implementing IPsec for Mobile IP Applications</a></li><li>• <a href="#">Implementing IPsec for L2TP Applications</a></li><li>• <a href="#">Transform Set Configuration</a></li><li>• <a href="#">ISAKMP Policy Configuration</a></li><li>• <a href="#">ISAKMP Crypto Map Configuration</a></li><li>• <a href="#">Dynamic Crypto Map Configuration</a></li><li>• <a href="#">Manual Crypto Map Configuration</a></li><li>• <a href="#">Crypto Map and Interface Association</a></li><li>• <a href="#">FA Services Configuration to Support IPsec</a></li><li>• <a href="#">HA Service Configuration to Support IPsec</a></li><li>• <a href="#">RADIUS Attributes for IPsec-based Mobile IP Applications</a></li><li>• <a href="#">LAC Service Configuration to Support IPsec</a></li><li>• <a href="#">Subscriber Attributes for L2TP Application IPsec Support</a></li><li>• <a href="#">Redundant IPsec Tunnel Fail-Over</a></li><li>• <a href="#">Dead Peer Detection (DPD) Configuration</a></li></ul>



# IPSec Terminology

There are four items related to IPSec support on the system that must be understood prior to beginning configuration. They are:

- Crypto Access Control List (ACL)
- Transform Set
- ISAKMP Policy
- Crypto Map

## Crypto Access Control List (ACL)

As described in the *IP Access Control Lists* chapter of this guide, ACLs on the system define rules, usually permissions, for handling subscriber data packets that meet certain criteria. Crypto ACLs, however, define the criteria that must be met in order for a subscriber data packet to be routed over an IPSec tunnel.

Unlike other ACLs that are applied to interfaces, contexts, or one or more subscribers, crypto ACLs are matched with crypto maps. In addition, crypto ACLs contain only a single rule while other ACL types can consist of multiple rules.

Prior to routing, the system examines the properties of each subscriber data packet. If the packet properties match the criteria specified in the crypto ACL, the system will initiate the IPSec policy dictated by the crypto map.

## Transform Set

Transform Sets are used to define IPSec security associations (SAs). IPSec SAs specify the IPSec protocols to use to protect packets.

Transform sets are used during Phase 2 of IPSec establishment. In this phase, the system and a peer security gateway negotiate one or more transform sets (IPSec SAs) containing the rules for protecting packets. This negotiation ensures that both peers can properly protect and process the packets.

## ISAKMP Policy

Internet Security Association Key Management Protocol (ISAKMP) policies are used to define Internet Key Exchange (IKE) SAs. The IKE SAs dictate the shared security parameters (i.e. which encryption parameters to use, how to authenticate the remote peer, etc.) between the system and a peer security gateway.

During Phase 1 of IPSec establishment, the system and a peer security gateway negotiate IKE SAs. These SAs are used to protect subsequent communications between the peers including the IPSec SA negotiation process.

## Crypto Map

Crypto Maps define the tunnel policies that determine how IPSec is implemented for subscriber data packets.

There are three types of crypto maps supported by the system. They are:

- Manual crypto maps

- ISAKMP crypto maps
- Dynamic crypto maps

## Manual Crypto Maps

These are static tunnels that use pre-configured information (including security keys) for establishment. Because they rely on statically configured information, once created, the tunnels never expire; they exist until their configuration is deleted.

Manual crypto maps define the peer security gateway to establish a tunnel with, the security keys to use to establish the tunnel, and the IPSec SA to be used to protect data sent/received over the tunnel. Additionally, manual crypto maps are applied to specific system interfaces.



**Important:** Because manual crypto map configurations require the use of static security keys (associations), they are not as secure as crypto maps that rely on dynamically configured keys. Therefore, it is recommended that they only be configured and used for testing purposes.

## ISAKMP Crypto Maps

These tunnels are similar to manual crypto maps in that they require some statically configured information such as the IP address of a peer security gateway and that they are applied to specific system interfaces.

However, ISAKMP crypto maps offer greater security because they rely on dynamically generated security associations through the use of the Internet Key Exchange (IKE) protocol.

When ISAKMP crypto maps are used, the system uses the pre-shared key configured for map as part of the Diffie-Hellman (D-H) exchange with the peer security gateway to initiate Phase 1 of the establishment process. Once the exchange is complete, the system and the security gateway dynamically negotiate IKE SAs to complete Phase 1. In Phase 2, the two peers dynamically negotiate the IPSec SAs used to determine how data traversing the tunnel will be protected.

## Dynamic Crypto Maps

These tunnels are used for protecting L2TP-encapsulated data between the system and an LNS/security gateway or Mobile IP data between an FA service configured on one system and an HA service configured on another.

The system determines when to implement IPSec for L2TP-encapsulated data either through attributes returned upon successful authentication for attribute based tunneling, or through the configuration of the LAC service used for compulsory tunneling.

The system determines when to implement IPSec for Mobile IP based on RADIUS attribute values as well as the configurations of the FA and HA service(s).

# Implementing IPsec for PDN Access Applications

This section provides information on the following topics:

- [How the IPsec-based PDN Access Configuration Works](#)
- [Configuring IPsec Support for PDN Access](#)

In covering these topics, this section assumes that ISAKMP crypto maps are configured/used as opposed to manual crypto maps.

## How the IPsec-based PDN Access Configuration Works

The following figure and the text that follows describe how sessions accessing a PDN using IPsec are processed by the system.

Figure 53. IPsec PDN Access Processing

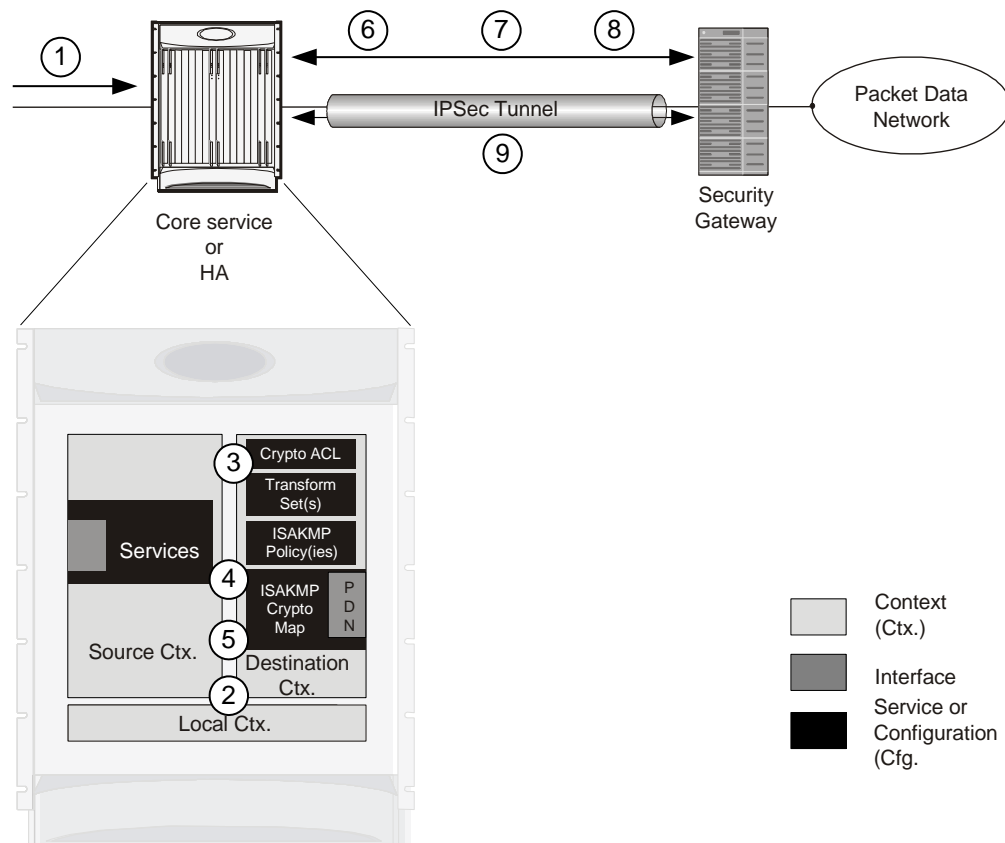


Table 23. IPsec PDN Access Processing

Step	Description
------	-------------

Step	Description
1.	A subscriber session or PDP context Request, in GGSN service, arrives at the system.
2.	The system processes the subscriber session or request as it would typically.
3.	Prior to routing the session packets, the system compares them against configured Access Control Lists (ACLs).
4.	The system determines that the packet matches the criteria of an ACL that is associated with a configured crypto map.
5.	From the crypto map, the system determines the following: <ul style="list-style-type: none"> <li>• The map type, in this case ISAKMP</li> <li>• The pre-shared key used to initiate the Internet Key Exchange (IKE) and the IKE negotiation mode</li> <li>• The IP address of the security gateway</li> <li>• Whether perfect forward secrecy (PFS) should be enabled for the IPsec SA and if so, what group should be used</li> <li>• IPsec SA lifetime parameters</li> <li>• The name of a configured transform set defining the IPsec SA</li> </ul>
6.	To initiate the IKE SA negotiation, the system performs a Diffie-Hellman exchange of the pre-shared key specified in the crypto map with the specified peer security gateway.
7.	The system and the security gateway negotiate an ISAKMP policy (IKE SA) to use to protect further communications.
8.	Once the IKE SA has been negotiated, the system negotiates an IPsec SA with the security gateway using the transform method specified in the transform sets.
9.	Once the IPsec SA has been negotiated, the system protects the data according to the IPsec SAs established during step 8 and sends it over the IPsec tunnel.

## Configuring IPsec Support for PDN Access

This section provides a list of the steps required to configure IPsec functionality on the system in support of PDN access. Each step listed refers to a different section containing the specific instructions for completing the required procedure.



**Important:** These instructions assume that the system was previously configured to support subscriber data sessions either as a core service or an HA. In addition, parameters configured using this procedure must be configured in the same destination context on the system.

- Step 1** Configure one or more IP access control lists (ACLs) according to the information and instructions located in *IP Access Control Lists* chapter of this guide.
- Step 2** Configure one or more transform sets according to the instructions located in the [Transform Set Configuration](#) section of this chapter.
- Step 3** Configure one or more ISAKMP policies according to the instructions located in the [ISAKMP Policy Configuration](#) section of this chapter.

- Step 4** Configure an ipsec-isakmp crypto map according to the instructions located in the [ISAKMP Crypto Map Configuration](#) section of this chapter.
- Step 5** Apply the crypto map to an interface on the system according to the instructions located in the [Crypto Map and Interface Association](#) section of this chapter.
- Step 6** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

# Implementing IPSec for Mobile IP Applications

This section provides information on the following topics:

- [How the IPSec-based Mobile IP Configuration Works](#)
- [Configuring IPSec Support for Mobile IP](#)

## How the IPSec-based Mobile IP Configuration Works

The following figure and the text that follows describe how Mobile IP sessions using IPSec are processed by the system.

Figure 54. IPSec-based Mobile IP Session Processing

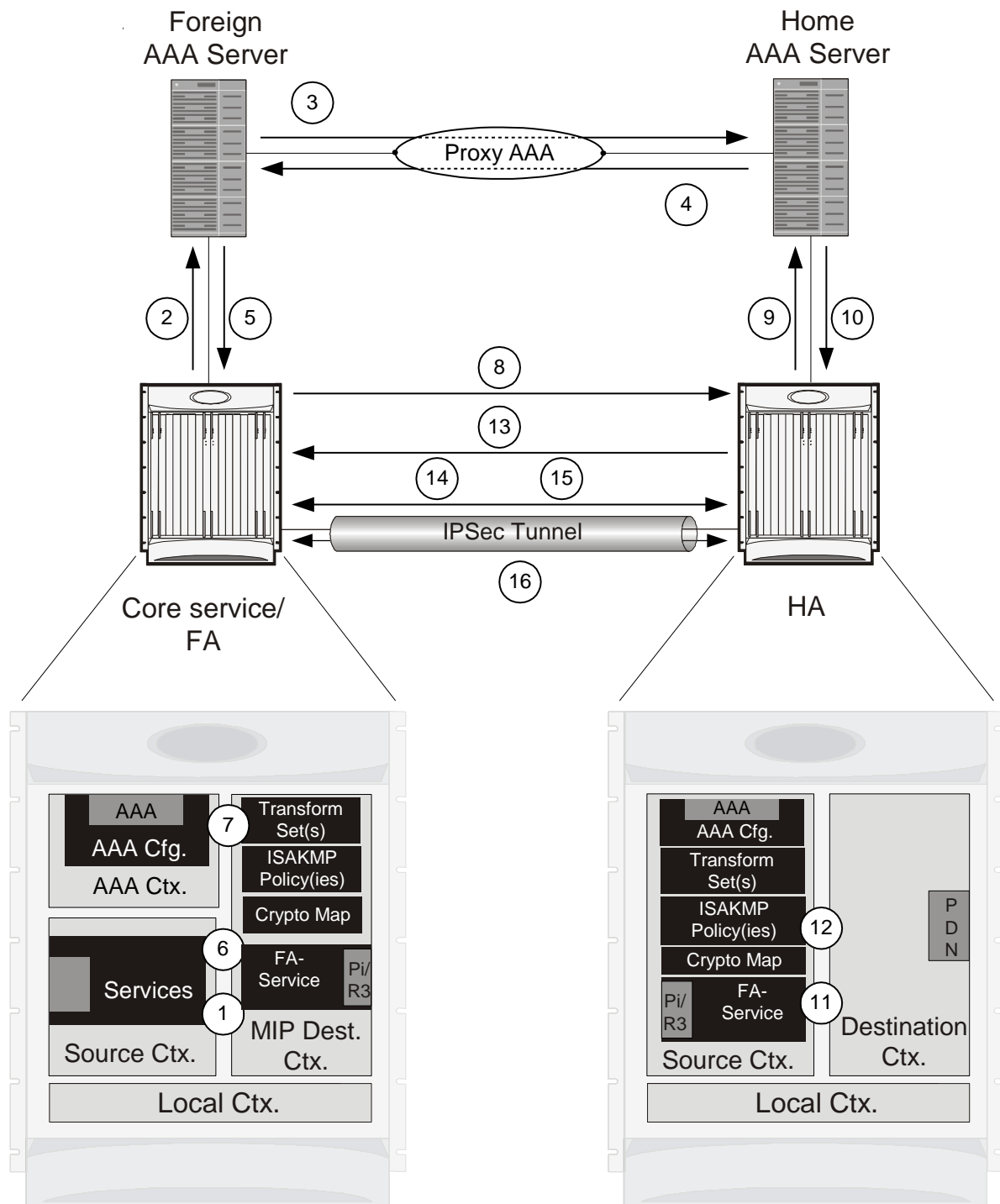


Table 24. IPSec-based Mobile IP Session Processing

Step	Description
------	-------------

Step	Description
1.	FA service receives a Mobile IP registration request from the mobile node.
2.	FA sends an Access-Request to the FAAA server with the 3GPP2-IKE-Secret-Request attribute equal to yes.
3.	The FAAA proxies the request to the HAAA.
4.	The HAAA returns an Access-Accept message including the following attributes: <ul style="list-style-type: none"> <li>• 3GPP2-Security-Level set to 3 for IPSec tunnels and registration messages</li> <li>• 3GPP2-MIP-HA-Address indicating the IP address of the HA that the FA is to communicate with.</li> <li>• 3GPP2-KeyId providing an identification number for the IKE secret (alternatively, the keys may be statically configured for the FA and/or HA)</li> <li>• 3GPP2-IKE-Secret indicating the pre-shared secret to use to negotiate the IKE SA</li> </ul>
5.	The FAAA passes the accept message to the FA with all of the attributes.
6.	The FA determines if an IPSec SA already exists based on the HA address supplied. If so, that SA will be used. If not, a new IPSec SA will be negotiated.
7.	The FA determines the appropriate crypto map to use for IPSec protection based on the HA address attribute. It does this by comparing the address received to those configured using the <b>isakmp peer-ha</b> command. From the crypto map, the system determines the following: <ul style="list-style-type: none"> <li>• The map type, in this case dynamic</li> <li>• Whether perfect forward secrecy (PFS) should be enabled for the IPSec SA and if so, what group should be used</li> <li>• IPSec SA lifetime parameters</li> <li>• The name of one or more configured transform set defining the IPSec SA</li> </ul>
8.	To initiate the IKE SA negotiation, the FA performs a Diffie-Hellman (D-H) exchange of the ISAKMP secret specified in the IKE secret attribute with the peer HA dictated by the HA address attribute. Included in the exchange is the Key ID received from the HAAA.
9.	Upon receiving the exchange, the HA sends an access request to the HAAA with the following attributes: <ul style="list-style-type: none"> <li>• 3GPP2-S-Request (note that this attribute is not used if the IPSec keys are statically configured)</li> <li>• 3GPP2-User-name (the username specified is the IP addresses of the FA and HA).</li> </ul> The password used in the access request is the RADIUS shared secret.
10.	The HAAA returns an Access-Accept message to the HA with the following attributes: <ul style="list-style-type: none"> <li>• 3GPP2-S indicating the “S” secret used to generate the HA’s response to the D-H exchange</li> <li>• 3GPP2-S-Lifetime indicating the length of time that the “S” secret is valid</li> <li>• 3GPP2-Security-Level set to 3 for IPSec tunnels and registration messages (optional)</li> </ul>



Step	Description
11.	The HA determines the appropriate crypto map to use for IPsec protection based on the FA's address. It does this by comparing the address received to those configured using the <code>isakmp peer-fa</code> command. From the crypto map, the system determines the following: <ul style="list-style-type: none"> <li>• The map type, in this case dynamic</li> <li>• Whether perfect forward secrecy (PFS) should be enabled for the IPsec SA and if so, what group should be used</li> <li>• IPsec SA lifetime parameters</li> <li>• The name of one or more configured transform set defining the IPsec SA</li> </ul>
12.	The HA creates a response to the D-H exchange using the "S" secret and the Key ID sent by the FA.
13.	The HA sends IKE SA negotiation D-H exchange response to the FA.
14.	The FA and the HA negotiate an ISAKMP (IKE) policy to use to protect further communications.
15.	Once the IKE SA has been negotiated, the system negotiates an IPsec SA with the security gateway using the transform method specified in the transform sets.
16.	Once the IPsec SA has been negotiated, the system protects the data according to the IPsec SAs established during step 15 and sends it over the IPsec tunnel.



**Important:** Once an IPsec tunnel is established between an FA and HA for a particular subscriber, all new Mobile IP sessions using the same FA and HA are passed over the tunnel regardless of whether or not IPsec is supported for the new subscriber sessions. Data for existing Mobile IP sessions is unaffected.

## Configuring IPsec Support for Mobile IP

This section provides a list of the steps required to configure IPsec functionality on the system in support of Mobile IP. Each step listed refers to a different section containing the specific instructions for completing the required procedure.



**Important:** These instructions assume that the systems were previously configured to support subscriber data sessions either as an FA or an HA.

- Step 1** Configure one or more transform sets for the FA system according to the instructions located in the [Transform Set Configuration](#) section of this chapter.
- The transform set(s) must be configured in the same context as the FA service.
- Step 2** Configure one or more ISAKMP policies for the FA system according to the instructions located in the [ISAKMP Policy Configuration](#) section of this chapter.
- The ISAKMP policy(ies) must be configured in the same context as the FA service.
- Step 3** Configure an ipsec-isakmp crypto map for the FA system according to the instructions located in the [Dynamic Crypto Map Configuration](#) section of this chapter.
- The crypto map(s) must be configured in the same context as the FA service.

- Step 4** Optional. Configure DPD for the FA to help prevent IPSec tunnel state mismatches between the FA and HA according to the instructions located in the [Dead Peer Detection \(DPD\) Configuration](#) section of this chapter.



**Important:** Though the use of DPD is optional, it is recommended in order to ensure service availability.

- Step 5** Configure the FA Service or the FA system according to the instructions located in the [FA Services Configuration to Support IPSec](#) section of this chapter.
- Step 6** Configure one or more transform sets for the HA system according to the instructions located in the [Transform Set Configuration](#) section of this chapter.  
The transform set(s) must be configured in the same context as the HA service.
- Step 7** Configure one or more ISAKMP policies or the HA system according to the instructions located in the [ISAKMP Policy Configuration](#) section of this chapter.  
The ISAKMP policy(ies) must be configured in the same context as the HA service.
- Step 8** Configure an ipsec-isakmp crypto map or the HA system according to the instructions located in the [Dynamic Crypto Map Configuration](#) section of this chapter.  
The crypto map(s) must be configured in the same context as the HA service.
- Step 9** Optional. Configure DPD for the HA to help prevent IPSec tunnel state mismatches between the FA and HA according to the instructions located in the [Dead Peer Detection \(DPD\) Configuration](#) section of this chapter.



**Important:** Though the use of DPD is optional, it is recommended in order to ensure service availability.

- Step 10** Configure the HA Service or the HA system according to the instructions located in the section of this chapter.
- Step 11** Configure the required attributes for RADIUS-based subscribers according to the information located in the [RADIUS Attributes for IPSec-based Mobile IP Applications](#) section of this chapter.
- Step 12** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

# Implementing IPsec for L2TP Applications

This section provides information on the following topics:

- [How IPsec is Used for Attribute-based L2TP Configurations](#)
- [Configuring Support for L2TP Attribute-based Tunneling with IPsec](#)
- [How IPsec is Used for PDSN Compulsory L2TP Configurations](#)
- [Configuring Support for L2TP PDSN Compulsory Tunneling with IPsec](#)
- [How IPsec is Used for L2TP Configurations on the GGSN](#)
- [Configuring GGSN Support for L2TP Tunneling with IPsec](#)

## How IPsec is Used for Attribute-based L2TP Configurations

The following figure and the text that follows describe how IPsec-encrypted attribute-based L2TP sessions are processed by the system.

Figure 55. Attribute-based L2TP, IPsec-Encrypted Session Processing

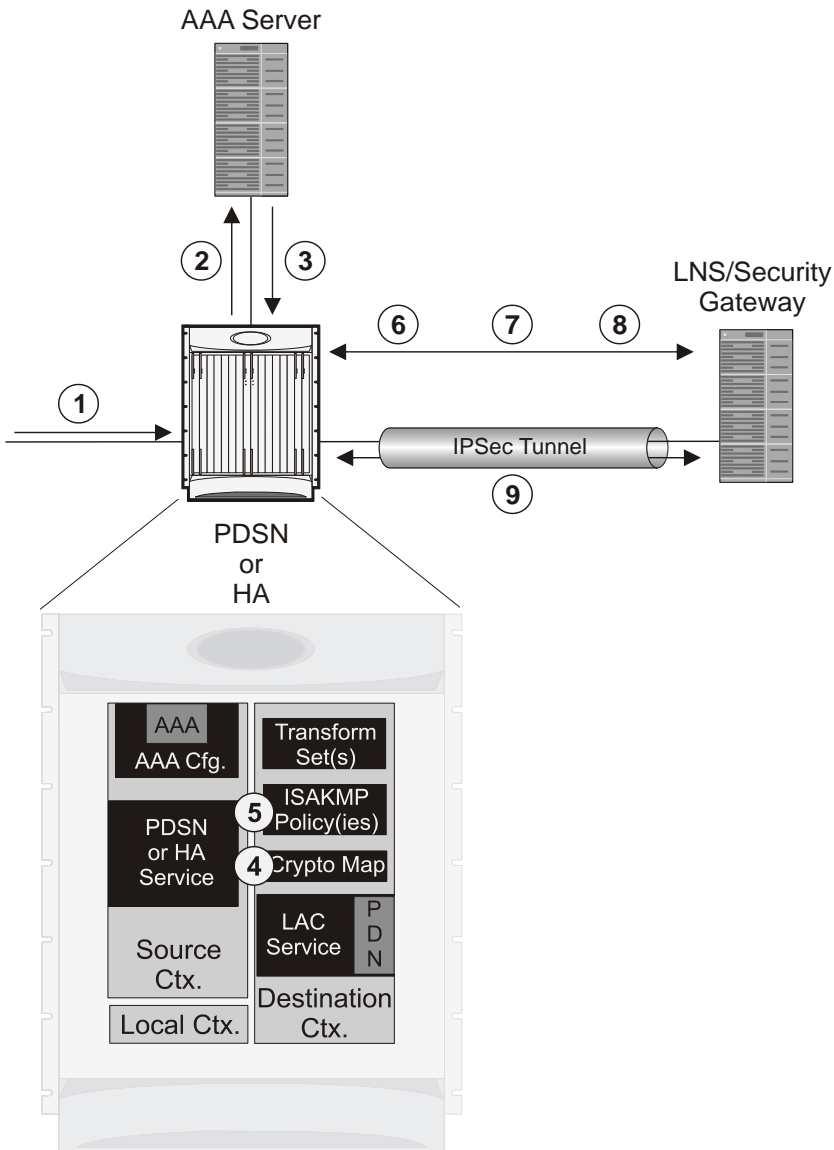


Table 25. Attribute-based L2TP, IPsec-Encrypted Session Processing

Step	Description
1.	A subscriber session arrives at the system.
2.	The system attempts to authenticate the subscriber with the AAA server.
3.	The profile attributes returned upon successful authentication by the AAA server indicate that session data is to be tunneled using L2TP. In addition, attributes specifying a crypto map name and ISAKMP secret are also supplied indicating that IP security is also required.
4.	The system determines that the crypto map name supplied matches a configured crypto map.

Step	Description
5.	From the crypto map, the system determines the following: <ul style="list-style-type: none"> <li>• The map type, in this case dynamic</li> <li>• Whether perfect forward secrecy (PFS) should be enabled for the IPsec SA and if so, what group should be used</li> <li>• IPsec SA lifetime parameters</li> <li>• The name of one or more configured transform set defining the IPsec SA</li> </ul>
6.	To initiate the IKE SA negotiation, the system performs a Diffie-Hellman exchange of the ISAKMP secret specified in the profile attribute with the specified peer LNS/security gateway.
7.	The system and the LNS/security gateway negotiate an ISAKMP (IKE) policy to use to protect further communications.
8.	Once the IKE SA has been negotiated, the system negotiates an IPsec SA with the LNS/security gateway using the transform method specified in the transform sets.
9.	Once the IPsec SA has been negotiated, the system protects the L2TP encapsulated data according to the IPsec SAs established during step 9 and sends it over the IPsec tunnel.

## Configuring Support for L2TP Attribute-based Tunneling with IPsec

This section provides a list of the steps required to configure IPsec functionality on the system in support of attribute-based L2TP tunneling. Each step listed refers to a different section containing the specific instructions for completing the required procedure.



**Important:** These instructions assume that the system was previously configured to support subscriber data sessions and L2TP tunneling either as a PDSN or an HA. In addition, with the exception of subscriber attributes, all other parameters configured using this procedure must be configured in the same destination context on the system as the LAC service.

- Step 1** Configure one or more transform sets according to the instructions located in the [Transform Set Configuration](#) section of this chapter.
- Step 2** Configure one or more ISAKMP policies according to the instructions located in the [ISAKMP Policy Configuration](#) section of this chapter.
- Step 3** Configure an ipsec-isakmp crypto map according to the instructions located in the [Dynamic Crypto Map Configuration](#) section of this chapter.
- Step 4** Configure the subscriber profile attributes according to the instructions located in the [Subscriber Attributes for L2TP Application IPsec Support](#) section of this chapter.
- Step 5** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

## How IPsec is Used for PDSN Compulsory L2TP Configurations

The following figure and the text that follows describe how IPsec-encrypted PDSN compulsory L2TP sessions are processed by the system.

Figure 56. PDSN Compulsory L2TP, IPsec-Encrypted Session Processing

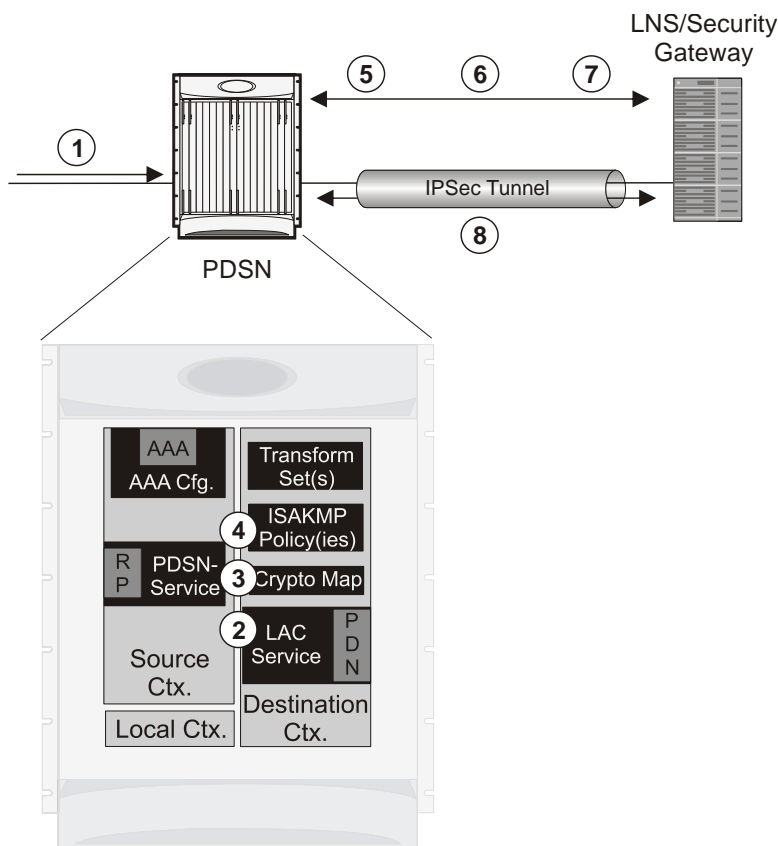


Table 26. PDSN Compulsory L2TP, IPsec-Encrypted Session Processing

Step	Description
1.	A subscriber session arrives at a PDSN service on the system that is configured to perform compulsory tunneling. The system uses the LAC service specified in the PDSN service's configuration.
2.	The LAC service dictates the peer LNS to use and also specifies the following parameters indicating that IP security is also required: <ul style="list-style-type: none"> <li>• Crypto map name</li> <li>• ISAKMP secret</li> </ul>
3.	The system determines that the crypto map name supplied matches a configured crypto map.

Step	Description
4.	From the crypto map, the system determines the following: <ul style="list-style-type: none"> <li>• The map type, in this case dynamic</li> <li>• Whether perfect forward secrecy (PFS) should be enabled for the IPSec SA and if so, what group should be used</li> <li>• IPSec SA lifetime parameters</li> <li>• The name of one or more configured transform set defining the IPSec SA</li> </ul>
5.	To initiate the IKE SA negotiation, the system performs a Diffie-Hellman exchange of the ISAKMP secret specified by the attribute with the specified peer LNS/security gateway.
6.	The system and the LNS/security gateway negotiate an ISAKMP policy (IKE SA) to use to protect further communications.
7.	Once the IKE SA has been negotiated, the system negotiates an IPSec SA with the LNS/security gateway.
8.	Once the IPSec SA has been negotiated, the system protects the L2TP encapsulated data according to the rules specified in the transform set and sends it over the IPSec tunnel.

## Configuring Support for L2TP PDSN Compulsory Tunneling with IPSec

This section provides a list of the steps required to configure IPSec functionality on the system in support of PDSN compulsory L2TP tunneling. Each step listed refers to a different section containing the specific instructions for completing the required procedure.



**Important:** These instructions assume that the system was previously configured to support PDSN compulsory tunneling subscriber data sessions. In addition, all parameters configured using this procedure must be configured in the same destination context on the system as the LAC service.

- Step 1** Configure one or more transform sets according to the instructions located in the [Transform Set Configuration](#) section of this chapter.
- Step 2** Configure one or more ISAKMP policies according to the instructions located in the [ISAKMP Policy Configuration](#) section of this chapter.
- Step 3** Configure an ipsec-isakmp crypto map according to the instructions located in the [Dynamic Crypto Map Configuration](#) section of this chapter.
- Step 4** Configure the subscriber profile attributes according to the instructions located in the [Subscriber Attributes for L2TP Application IPSec Support](#) section of this chapter.
- Step 5** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

## How IPsec is Used for L2TP Configurations on the GGSN

The following figure and the text that follows describe how IPsec-encrypted attribute-based L2TP sessions are processed by the system.

Figure 57. GGSN PDP Context Processing with IPsec-Encrypted L2TP

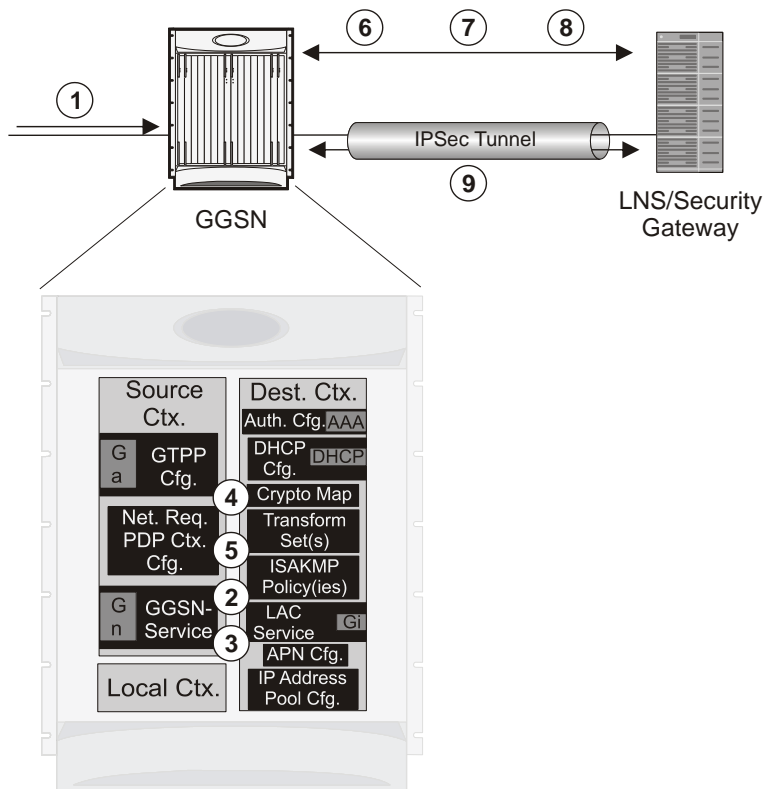


Table 27. GGSN PDP Context Processing with IPsec-Encrypted L2TP

Step	Description
1.	A subscriber session/PDP Context Request arrives at the system.
2.	The configuration of the APN accessed by the subscriber indicates that session data is to be tunneled using L2TP. In addition, attributes specifying a crypto map name and ISAKMP secret are also supplied indicating that IP security is also required.
3.	The system determines that the crypto map name supplied matches a configured crypto map.
4.	From the crypto map, the system determines the following: <ul style="list-style-type: none"> <li>The map type, in this case dynamic</li> <li>Whether perfect forward secrecy (PFS) should be enabled for the IPsec SA and if so, what group should be used</li> <li>IPsec SA lifetime parameters</li> <li>The name of one or more configured transform set defining the IPsec SA</li> </ul>



Step	Description
5.	To initiate the IKE SA negotiation, the system performs a Diffie-Hellman exchange of the ISAKMP secret specified in the profile attribute with the specified peer LNS/security gateway.
6.	The system and the LNS/security gateway negotiate an ISAKMP (IKE) policy to use to protect further communications.
7.	Once the IKE SA has been negotiated, the system negotiates an IPsec SA with the LNS/security gateway using the transform method specified in the transform sets.
8.	Once the IPsec SA has been negotiated, the system protects the L2TP encapsulated data according to the IPsec SAs established during step 9 and sends it over the IPsec tunnel.

## Configuring GGSN Support for L2TP Tunneling with IPsec

This section provides a list of the steps required to configure the GGSN to encrypt L2TP tunnels using IPSEC. Each step listed refers to a different section containing the specific instructions for completing the required procedure.



**Important:** These instructions assume that the system was previously configured to support subscriber PDP contexts and L2TP tunneling either as a GGSN. In addition, all parameters configured using this procedure must be configured in the same destination context on the system as the LAC service.

- Step 1** Configure one or more transform sets according to the instructions located in the [Transform Set Configuration](#) section of this chapter.
- Step 2** Configure one or more ISAKMP policies according to the instructions located in the [ISAKMP Policy Configuration](#) section of this chapter.
- Step 3** Configure an ipsec-isakmp crypto map according to the instructions located in the [Dynamic Crypto Map Configuration](#) section of this chapter.
- Step 4** Configure APN support for encrypting L2TP tunnels using IPsec according to the instructions located in the [APN Template Configuration to Support L2TP](#) section of this chapter.
- Step 5** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command `save configuration`. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

# Transform Set Configuration

This section provides instructions for configuring transform sets on the system.



**Important:** This section provides the minimum instruction set for configuring transform set on your system. For more information on commands that configure additional parameters and options, refer to the *Context Configuration Mode Commands* and *Crypto Transform Configuration Mode* chapters in the *Command Line Interface Reference*.

To configure the crypto transform set for IPSec:

- Step 1** Configure crypto transform set by applying the example configuration in the [Configuring Transform Set](#) section.
- Step 2** Verify your Crypto Transform Set configuration by following the steps in the [Verifying the Crypto Transform Set Configuration](#) section.
- Step 3** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

## Configuring Transform Set

Use the following example to create the crypto transform set on your system:

```
configure

context <ctxt_name>

    crypto ipsec transform-set <transform_name> ah hmac { md5-96 | none | sha1-96 } esp
hmac { { md5-96 | none | sha1-96 } { cipher {des-cbc | 3des-cbc | aes-cbc } | none }

    mode { transport | tunnel }

end
```

Notes:

- <ctxt\_name> is the system context in which you wish to create and configure the crypto transform set(s).
- <transform\_name> is the name of the crypto transform set in the current context that you want to configure for IPSec configuration.
- For more information on parameters, refer to the *IPSec Transform Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

## Verifying the Crypto Transform Set Configuration

These instructions are used to verify the crypto transform set(s) was/were configured.

- Step 1** Verify that your header crypto transform set configurations by entering the following command in Exec Mode in specific context:

```
show crypto transform-set transform_name
```

This command produces an output similar to that displayed below using the configuration of a transform set named test1.

```
Transform-Set test1 :  
  
AH : none  
  
ESP :hmac md5-96, 3des-cbc  
  
Encaps Mode: TUNNEL
```

# ISAKMP Policy Configuration

This section provides instructions for configuring ISAKMP policies on the system. ISAKMP policy configuration is only required if the crypto map type is either ISAKMP or Dynamic.



**Important:** This section provides the minimum instruction set for configuring ISAKMP policies on the system. For more information on commands that configure additional parameters and options, refer to the *Context Configuration Mode Commands* and *ISAKMP Configuration Mode Commands* chapters in the *Command Line Interface Reference*.

To configure the ISAKMP policy for IPsec:

- Step 1** Configure crypto transform set by applying the example configuration in the [Configuring ISAKMP Policy](#) section.
- Step 2** Verify your ISAKMP policy configuration by following the steps in the [Verifying the ISAKMP Policy Configuration](#) section.
- Step 3** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

## Configuring ISAKMP Policy

Use the following example to create the ISAKMP policy on your system:

**configure**

```
context <ctxt_name>

    ikev1 policy <priority>

        encryption { 3des-cbc | des-cbc }

        hash { md5 | sha1 }

        group { 1 | 2 | 3 | 4 | 5 }

        lifetime <time>

    end
```

Notes:

- <ctxt\_name> is the system context in which you wish to create and configure the ISAKMP policy.
- <priority> dictates the order in which the ISAKMP policies are proposed when negotiating IKE SAs.
- For more information on parameters, refer to the *ISAKMP Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

## Verifying the ISAKMP Policy Configuration

These instructions are used to verify the ISAKMP policy configuration.

**Step 1** Verify that your ISAKMP policy configuration by entering the following command in Exec Mode in specific context:

```
show crypto isakmp policy priority
```

This command produces an output similar to that displayed below that displays the configuration of an ISAKMP policy with priority 1.

```
1 ISAKMP Policies are configured

Priority : 1

Authentication Method : preshared-key

Lifetime : 120 seconds

IKE group : 5

hash : md5

encryption : 3des-cbc
```



**Caution:** Modification(s) to an existing ISAKMP policy configuration will not take effect until the related security association has been cleared. Refer to the **clear crypto security-association** command located in the *Exec Mode Commands* chapter of the *Command Line Interface Reference* for more information.

---

# ISAKMP Crypto Map Configuration

This section provides instructions for configuring ISAKMP crypto maps.



**Important:** This section provides the minimum instruction set for configuring ISAKMP crypto maps on the system. For more information on commands that configure additional parameters and options, refer to the *Context Configuration Mode Commands* and *Crypto Map ISAKMP Configuration Mode* chapters in the *Command Line Interface Reference*.

To configure the ISAKMP crypto maps for IPsec:

- Step 1** Configure ISAKMP crypto map by applying the example configuration in the [Configuring ISAKMP Crypto Maps](#) section.
- Step 2** Verify your ISAKMP crypto map configuration by following the steps in the [Verifying the ISAKMP Crypto Map Configuration](#) section.
- Step 3** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

## Configuring ISAKMP Crypto Maps

Use the following example to create the ISAKMP crypto map on your system:

**configure**

```
context <ctxt_name>

  crypto map <map_name> ipsec-isakmp

    set peer <agw_address>

    set isakmp preshared-key <isakmp_key>

    set mode { aggressive | main }

    set pfs { group1 | group2 | group5 }

    set transform-set <transform_name>

    match address <acl_name> [ preference ]

    match crypto-group <group_name> { primary | secondary }

  end
```

Notes:

- <ctxt\_name> is the system context in which you wish to create and configure the ISAKMP crypto maps.
- <map\_name> is name by which the ISAKMP crypto map will be recognized by the system.

- `<acl_name>` is name of the pre-configured ACL. It is used for configurations not implementing the IPSec Tunnel Failover feature and match the crypto map to a previously defined crypto ACL. This is an optional parameter.
- `<group_name>` is name of the Crypto group configured in the same context. It is used for configurations using the IPSec Tunnel Failover feature. This is an optional parameter. For more information, refer to the [Redundant IPSec Tunnel Fail-Over](#) section of this chapter.
- For more information on parameters, refer to the *Crypto Map ISAKMP Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

## Verifying the ISAKMP Crypto Map Configuration

These instructions are used to verify the ISAKMP crypto map configuration.

- Step 1** Verify that your ISAKMP crypto map configurations by entering the following command in Exec Mode in specific context:

```
show crypto map [ tag map_name | type ipsec-isakmp ]
```

This command produces an output similar to that displayed below that displays the configuration of a crypto map named `test_map2`.

```
Map Name : test_map2

=====

Payload :

crypto_acl2: permit tcp host 10.10.2.12 neq 35 any

Crypto map Type : ISAKMP

IKE Mode : MAIN

IKE pre-shared key : 3fd32rf09svc

Perfect Forward Secrecy : Group2

Hard Lifetime :

28800 seconds

4608000 kilobytes

Number of Transforms: 1

Transform : test1

AH : none


ESP: md5 3des-cbc

Encaps mode: TUNNEL
```

Local Gateway: Not Set

Remote Gateway: 192.168.1.1

---

 **Caution:** Modification(s) to an existing ISAKMP crypto map configuration will not take effect until the related security association has been cleared. Refer to the `clear crypto security-association` command located in the *Exec Mode Commands* chapter of the *Command Line Interface Reference* for more information.

---



# Dynamic Crypto Map Configuration

This section provides instructions for configuring dynamic crypto maps. Dynamic crypto maps should only be configured in support of L2TP or Mobile IP applications.



**Important:** This section provides the minimum instruction set for configuring dynamic crypto maps on the system. For more information on commands that configure additional parameters and options, refer to the *Context Configuration Mode Commands* and *Crypto Map Dynamic Configuration Mode* chapters in the *Command Line Interface Reference*.

To configure the dynamic crypto maps for IPsec:

- Step 1** Configure dynamic crypto maps by applying the example configuration in the [Configuring Dynamic Crypto Maps](#) section.
- Step 2** Verify your dynamic crypto map configuration by following the steps in the [Verifying the Dynamic Crypto Map Configuration](#) section.
- Step 3** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

## Configuring Dynamic Crypto Maps

Use the following example to create the crypto transform set on your system:

```
configure

context <ctxt_name>

    crypto map <map_name> ipsec-dynamic

        set pfs { group1 | group2 | group5 }

        set transform-set <transform_name>

    end
```

Notes:

- <ctxt\_name> is the system context in which you wish to create and configure the dynamic crypto maps.
- <map\_name> is name by which the dynamic crypto map will be recognized by the system.
- For more information on parameters, refer to the *Crypto Map Dynamic Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

## Verifying the Dynamic Crypto Map Configuration

These instructions are used to verify the dynamic crypto map configuration.

**Step 1** Verify that your dynamic crypto map configurations by entering the following command in Exec Mode in specific context:

```
show crypto map [ tag map_name | type ipsec-dynamic ]
```

This command produces an output similar to that displayed below using the configuration of a dynamic crypto map named test\_map3.

```
Map Name : test_map3

=====

Crypto map Type : ISAKMP (Dynamic)

IKE Mode : MAIN

IKE pre-shared key :

Perfect Forward Secrecy : Group2

Hard Lifetime :

28800 seconds

4608000 kilobytes

Number of Transforms: 1

Transform : test1

AH : none

ESP: md5 3des-cbc

Encaps mode: TUNNEL

Local Gateway: Not Set

Remote Gateway: Not Set
```





**Caution:** Modification(s) to an existing dynamic crypto map configuration will not take effect until the related security association has been cleared. Refer to the **clear crypto security-association** command located in the *Exec Mode Commands* chapter of the *Command Line Interface Reference* for more information.

---

# Manual Crypto Map Configuration

This section provides instructions for configuring manual crypto maps on the system.

 **Important:** Because manual crypto map configurations require the use of static security keys (associations), they are not as secure as crypto maps that rely on dynamically configured keys. Therefore, it is recommended that they only be configured and used for testing purposes.

 **Important:** This section provides the minimum instruction set for configuring manual crypto maps on the system. For more information on commands that configure additional parameters and options, refer to the *Context Configuration Mode Commands* and *Crypto Map Manual Configuration Mode* chapters in the *Command Line Interface Reference*.

To configure the manual crypto maps for IPSec:

- Step 1** Configure manual crypto map by applying the example configuration in the [Configuring Manual Crypto Maps](#) section.
- Step 2** Verify your manual crypto map configuration by following the steps in the [Verifying the Manual Crypto Map Configuration](#) section.
- Step 3** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

## Configuring Manual Crypto Maps

Use the following example to create the manual crypto map on your system:

**configure**

```
context <ctxt_name>

  crypto map <map_name> ipsec-manual

    set peer <agw_address>

    match address <acl_name> [ preference ]

    set transform-set <transform_name>

    set session-key { inbound | outbound } { ah <ah_spi> [ encrypted ] key <ah_key>
| esp <esp_spi> [ encrypted ] cipher <encryption_key> [ encrypted ] authenticator
<auth_key> }

  end
```

Notes:

- <ctxt\_name> is the system context in which you wish to create and configure the manual crypto maps.

- `<map_name>` is name by which the manual crypto map will be recognized by the system.
- `<acl_name>` is name of the pre-configured ACL. It is used for configurations not implementing the IPsec Tunnel Failover feature and match the crypto map to a previously defined crypto ACL. This is an optional parameter.
- The length of the configured key must match the configured algorithm.
- `<group_name>` is name of the Crypto group configured in the same context. It is used for configurations using the IPsec Tunnel Failover feature. This is an optional parameter.
- For more information on parameters, refer to the *Crypto Map Manual Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

## Verifying the Manual Crypto Map Configuration

These instructions are used to verify the manual crypto map configuration.

- Step 1** Verify that your manual crypto map configurations by entering the following command in Exec Mode in specific context:

```
show crypto map [ tag map_name | type ipsec-manual ]
```

This command produces an output similar to that displayed below that displays the configuration of a crypto map named `test_map`.

```
Map Name : test_map

=====

Payload :

crypto_acl1: permit tcp host 1.2.3.4 gt 30 any

Crypto map Type : manual(static)

Transform : test1

Encaps mode: TUNNEL

Transmit Flow

Protocol : ESP

SPI : 0x102 (258)

Hmac : md5, key: 23d32d23cs89

Cipher : 3des-cbc, key: 1234asd3c3d

Receive Flow

Protocol : ESP


SPI : 0x101 (257) Hmac : md5, key: 008j90u3rjp
```

Cipher : 3des-cbc, key: sdfsdffasdf342d32

Local Gateway: Not Set

Remote Gateway: 192.168.1.40

---

 **Caution:** Modification(s) to an existing manual crypto map configuration will not take effect until the related security association has been cleared. Refer to the **clear crypto security-association** command located in the *Exec Mode Commands* chapter of the *Command Line Interface Reference* for more information.

---

## Crypto Map and Interface Association

This section provides instructions for applying manual or ISAKMP crypto maps to interfaces configured on the system. Dynamic crypto maps should not be applied to interfaces.



**Important:** This section provides the minimum instruction set for applying manual or ISAKMP crypto maps to an interface on the system. For more information on commands that configure additional parameters and options, refer to the *Command Line Interface Reference*.

To apply the crypto maps to an interface:

- Step 1** Configure a manual or ISAKMP crypto map by applying the example configuration in any of the following sections:
- Step 2** Apply desired crypto map to system interface by following the steps in the [Applying Crypto Map to an Interface](#) section
- Step 3** Verify your manual crypto map configuration by following the steps in the [Verifying the Interface Configuration with Crypto Map](#) section.
- Step 4** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

## Applying Crypto Map to an Interface

Use the following example to apply an existing crypto map to an interface on your system:

**configure**

```
context <ctxt_name>

    interface <interface_name>

        crypto-map <map_name>

    end
```

Notes:

- <ctxt\_name> is the system context in which the interface is configured to apply crypto map.
- <interface\_name> is the name of a specific interface configured in the context to which the crypto map will be applied.
- <map\_name> is name of the preconfigured ISAKMP or a manual crypto map.

## Verifying the Interface Configuration with Crypto Map

These instructions are used to verify the interface configuration with crypto map.

- Step 1** Verify that your interface is configured properly with crypto map by entering the following command in Exec Mode in specific context:

```
show configuration context ctxt_name | grep interface
```

The interface configuration aspect of the display should look similar to that shown below. In this example an interface named 20/6 was configured with a crypto map called isakmp\_map1.

```
interface 20/6  
  
ip address 192.168.4.10 255.255.255.0  
  
crypto-map isakmp_map1
```

## FA Services Configuration to Support IPSec

This section provides instructions for configuring FA services to support IPSec.

These instructions assume that the FA service was previously configured and system is ready to serve as an FA.



**Important:** This section provides the minimum instruction set for configuring an FA service to support IPSec on the system. For more information on commands that configure additional parameters and options, refer to the *Command Line Interface Reference*.

To configure the FA service to support IPSec:

- Step 1** Modify FA service configuration by following the steps in the [Modifying FA service to Support IPSec](#) section
- Step 2** Verify your FA service configuration by following the steps in the [Verifying the FA Service Configuration with IPSec](#) section.
- Step 3** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

## Modifying FA service to Support IPSec

Use the following example to modify FA service to support IPSec on your system:

**configure**

```
context <ctxt_name>

    fa-service <fa_svc_name>

        isakmp peer-ha <ha_address> crypto-map <map_name> [ secret <presared_secret> ]

        isakmp default crypto-map <map_name> [ secret <presared_secret> ]

    end
```

Notes:

- <ctxt\_name> is the system context in which the FA service is configured to support IPSec.
- <fa\_svc\_name> is name of the FA service for which you are configuring IPSec.
- <ha\_address> is IP address of the HA service to which FA service will communicate on IPSec.
- <map\_name> is name of the preconfigured ISAKMP or a manual crypto map.
- A default crypto map for the FA service to be used in the event that the AAA server returns an HA address that is not configured as an ISAKMP peer HA.
- For maximum security, the default crypto map should be configured in addition to peer-ha crypto maps instead of being used to provide IPSec SAs to all HAs. Note that once an IPSec tunnel is established between the FA and HA for a particular subscriber, all new Mobile IP sessions using the same FA and HA are passed over the



tunnel regardless of whether or not IPSec is supported for the new subscriber sessions. Data for existing Mobile IP sessions is unaffected.

## Verifying the FA Service Configuration with IPSec

These instructions are used to verify the FA service to support IPSec.

**Step 1** Verify that your FA service is configured properly with IPSec by entering the following command in Exec Mode in specific context:

```
show fa-service { name service_name | all }
```

The output of this command is a concise listing of FA service parameter settings configured on the system.

## HA Service Configuration to Support IPSec

This section provides instructions for configuring HA services to support IPSec.

These instructions assume that the HA service was previously configured and system is ready to serve as an HA.



**Important:** This section provides the minimum instruction set for configuring an HA service to support IPSec on the system. For more information on commands that configure additional parameters and options, refer to the *Command Line Interface Reference*.

To configure the HA service to support IPSec:

- Step 1** Modify HA service configuration by following the steps in the [Modifying HA service to Support IPSec](#) section
- Step 2** Verify your HA service configuration by following the steps in the [Verifying the HA Service Configuration with IPSec](#) section.
- Step 3** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

## Modifying HA service to Support IPSec

Use the following example to modify an existing HA service to support IPSec on your system:

**configure**

```
context <ctxt_name>

    ha-service <ha_svc_name>

        isakmp aaa-context <aaa_ctxt_name>

        isakmp peer-fa <fa_address> crypto-map <map_name> [ secret <presared_secret> ]

    end
```

Notes:

- <ctxt\_name> is the system context in which the FA service is configured to support IPSec.
- <ha\_svc\_name> is name of the HA service for which you are configuring IPSec.
- <fa\_address> is IP address of the FA service to which HA service will communicate on IPSec.
- <aaa\_ctxt\_name> name of the context through which the HA service accesses the HAAA server to fetch the IKE S Key and S Lifetime parameters.
- <map\_name> is name of the preconfigured ISAKMP or a manual crypto map.

## Verifying the HA Service Configuration with IPSec

These instructions are used to verify the HA service to support IPSec.

- Step 1** Verify that your HA service is configured properly with IPSec by entering the following command in Exec Mode in specific context:

```
show ha-service { name service_name | all }
```

The output of this command is a concise listing of HA service parameter settings configured on the system.

## RADIUS Attributes for IPSec-based Mobile IP Applications

As described in the [How the IPSec-based Mobile IP Configuration Works](#) section of this chapter, the system uses attributes stored in a subscriber's RADIUS profile to determine how IPSec should be implemented.

The table below lists the attributes that must be configured in the subscriber's RADIUS attributes to support IPSec for Mobile IP. These attributes are contained in the following dictionaries:

- 3GPP2
- 3GPP2-835
- Starent
- Starent-835
- Starent-VSA1
- Starent-VSA1-835

**Table 28. Attributes Used for Mobile IP IPSec Support**

Attribute	Description	Variable
3GPP2-Security-Level	This attribute indicates the type of security that the home network mandates on the visited network.	Integer value: <b>3</b> : Enables IPSec for tunnels and registration messages <b>4</b> : Disables IPSec
3GPP2 - KeyId	This attribute contains the opaque IKE Key Identifier for the FA/HA shared IKE secret.	Supported value for the first eight bytes is the network-order FA IP address in hexadecimal characters. Supported value for the next eight bytes is the network-order HA IP address in hexadecimal characters. Supported value for the final four bytes is a timestamp in network order, indicating when the key was created, and is the number of seconds since January 1, 1970, UTC.
3GPP2-IKE-Secret	This attribute contains the FA/HA shared secret for the IKE protocol. This attribute is salt-encrypted.	A binary string of 1 to 127 bytes.
3GPP2-S	This attribute contains the 'S' secret parameter used to make the IKE pre-shared secret.	A binary string of the value of 'S' consisting of 1 to 127 characters.
3GPP2- S-Lifetime	This attribute contains the lifetime of the 'S' secret parameter used to make the IKE pre-shared secret.	An integer in network order, indicating the time in seconds since January 1, 1970 00:00 UTC. Note that this is equivalent to the Unix operating system expression of time.

## LAC Service Configuration to Support IPSec

This section provides instructions for configuring LAC services to support IPSec.

**Important:** These instructions are required for compulsory tunneling. They should only be performed for attribute-based tunneling if the Tunnel-Service-Endpoint, the SN1-Tunnel-ISAKMP-Crypto-Map, or the SN1-Tunnel-ISAKMP-Secret are not configured in the subscriber profile.

These instructions assume that the LAC service was previously configured and system is ready to serve as an LAC server.

**Important:** This section provides the minimum instruction set for configuring an LAC service to support IPSec on the system. For more information on commands that configure additional parameters and options, refer to the *Command Line Interface Reference*.

To configure the LAC service to support IPSec:

- Step 1** Modify LAC service configuration by following the steps in the [Modifying LAC service to Support IPSec](#) section.
- Step 2** Verify your LAC service configuration by following the steps in the [Verifying the LAC Service Configuration with IPSec](#) section.
- Step 3** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

## Modifying LAC service to Support IPSec

Use the following example to modify an existing LAC service to support IPSec on your system:

**configure**

```
context <ctxt_name>

    lac-service <lac_svc_name>

        peer-lns <ip_address> [encrypted] secret <secret> [crypto-map <map_name> {
[encrypted] isakmp-secret <secret> } ] [ description <text> ] [ preference <integer>]

        isakmp aaa-context <aaa_ctxt_name>

        isakmp peer-fa <fa_address> crypto-map <map_name> [ secret <preshared_secret> ]

    end
```

Notes:

- <ctxt\_name> is the destination context where the LAC service is configured to support IPSec.

- `<lac_svc_name>` is name of the LAC service for which you are configuring IPSec.
- `<lms_address>` is IP address of the LMS node to which LAC service will communicate on IPSec.
- `<aaa_ctxt_name>` name of the context through which the HA service accesses the HAAA server to fetch the IKE S Key and S Lifetime parameters.
- `<map_name>` is name of the preconfigured ISAKMP or a manual crypto map.

## Verifying the LAC Service Configuration with IPSec

These instructions are used to verify the LAC service to support IPSec.

- Step 1** Verify that your LAC service is configured properly with IPSec by entering the following command in Exec Mode in specific context:

```
show lac-service nameservice_name
```

The output of this command is a concise listing of LAC service parameter settings configured on the system.

## Subscriber Attributes for L2TP Application IPSec Support

In addition to the subscriber profile attributes listed in the *RADIUS and Subscriber Profile Attributes Used* section of the *L2TP Access Concentrator* chapter in this guide, the table below lists the attributes required to support IPSec for use with attribute-based L2TP tunneling.

These attributes are contained in the following dictionaries:

- Starent
- Starent-835

**Table 29. Subscriber Attributes for IPSec encrypted L2TP Support**

RADIUS Attribute	Local SubscriberAttribute	Description	Variable
SN1-Tunnel-ISA-KMP-Crypto-Map	tunnel l2tp crypto-map	The name of a crypto map configured on the system.	A salt-encrypted ascii string specifying the crypto-map to use for this subscriber. It can be tagged, in which case it is treated as part of a tunnel group.
SN1 -Tunnel-ISA-KMP- Secret	tunnel l2tp crypto-map isakmp-secret	The pre-shared secret that will be used as part of the D-H exchange to negotiate an IKE SA.	A salt-encrypted string specifying the IKE secret. It can be tagged, in which case it is treated as part of a tunnel group.

## PDSN Service Configuration for L2TP Support

PDSN service configuration is required for compulsory tunneling and optional for attribute-based tunneling.

For attribute-based tunneling, a configuration error could occur such that upon successful authentication, the system determines that the subscriber session requires L2TP but can not determine the name of the context in which the appropriate LAC service is configured from the attributes supplied. As a precautionary, a parameter has been added to the PDSN service configuration options that will dictate the name of the context to use. It is strongly recommended that this parameter be configured.

This section contains instructions for modifying the PDSN service configuration for either compulsory or attribute-based tunneling.

These instructions assume that the PDSN service was previously configured and system is ready to serve as a PDSN.

This section provides the minimum instruction set for configuring an L2TP service on the PDSN system. For more information on commands that configure additional parameters and options, refer to the *Command Line Interface Reference*.

To configure the PDSN service to support L2TP:

- Step 1** Modify PDSN service to configure compulsory tunneling or attribute-based tunneling by applying the example configuration in any of the following sections:
- [Modifying PDSN service to Support Attribute-based L2TP Tunneling](#)
  - [Modifying PDSN service to Support Compulsory L2TP Tunneling](#)
- Step 2** Verify your LAC service configuration by following the steps in the [Verifying the PDSN Service Configuration for L2TP](#) section.
- Step 3** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

## Modifying PDSN service to Support Attribute-based L2TP Tunneling

Use the following example to modify an existing PDSN service to support attribute-based L2TP tunneling on your system:

```
configure

context <ctxt_name>

    pdsn-service <pdsn_svc_name>

        ppp tunnel-context <lac_ctxt_name>

    end
```

Notes:

- <ctxt\_name> is the destination context where the PDSN service is configured.



- `<pdsn_svc_name>` is name of the PDSN service for which you are configuring attribute-based L2TP tunneling.
- `<lac_ctxt_name>` is the name of the destination context where the LAC service is located.

## Modifying PDSN service to Support Compulsory L2TP Tunneling

Use the following example to modify an existing PDSN service to support compulsory L2TP tunneling on your system:

**configure**

```
context <ctxt_name>

  pdsn-service <pdsn_svc_name>

    ppp tunnel-context <lac_ctxt_name>

    ppp tunnel-type l2tp

  end
```

Notes:

- `<ctxt_name>` is the destination context where the PDSN service is configured.
- `<pdsn_svc_name>` is name of the PDSN service for which you are configuring attribute-based L2TP tunneling.
- `<lac_ctxt_name>` is name of the destination context where the LAC service is located.

## Verifying the PDSN Service Configuration for L2TP

These instructions are used to verify the PDSN service to support L2TP.

- Step 1** Verify that your PDSN service is configured properly with L2TP by entering the following command in Exec Mode in specific context:

```
show pdsn-service name service_name
```

The output of this command is a concise listing of PDSN service parameter settings configured on the system.

## Redundant IPSec Tunnel Fail-Over

The Redundant IPSec Tunnel Fail-Over functionality is included with the IPSec feature license and allows the configuration of a secondary ISAKMP crypto map-based IPSec tunnel over which traffic is routed in the event that the primary ISAKMP crypto map-based tunnel cannot be used.

This feature introduces the concept of crypto (tunnel) groups when using IPSec tunnels for access to packet data networks (PDNs). A crypto group consists of two configured ISAKMP crypto maps. Each crypto map defines the IPSec policy for a tunnel. In the crypto group, one tunnel serves as the primary, the other as the secondary (redundant). Note that the method in which the system determines to encrypt user data in an IPSec tunnel remains unchanged.

Group tunnels are perpetually maintained with IPSec Dead Peer Detection (DPD) packets exchanged with the peer security gateway.



**Important:** The peer security gateway must support RFC 3706 in order for this functionality to function properly.

---

When the system determines that incoming user data traffic must be routed over one of the tunnels in a group, the system automatically uses the primary tunnel until either the peer is unreachable (the IPSec DPD packets cease), or the IPSec tunnel fails to re-key. If the primary peer becomes unreachable, the system automatically begins to switch user traffic to the secondary tunnel. The system can be configured to either automatically switch user traffic back to the primary tunnel once the corresponding peer security gateway is reachable and the tunnel is configured, or require manual intervention to do so.

This functionality also supports the generation of Simple network Management Protocol (SNMP) notifications indicating the following conditions:

- **Primary Tunnel is down:** A primary tunnel that was previously "up" is now "down" representing an error condition.
- **Primary Tunnel is up:** A primary tunnel that was previously "down" is now "up".
- **Secondary tunnel is down:** A secondary tunnel that was previously "up" is now "down" representing an error condition.
- **Secondary Tunnel is up:** A secondary tunnel that was previously "down" is now "up".
- **Fail-over successful:** The switchover of user traffic was successful. This is generated for both primary-to-secondary and secondary-to-primary switchovers.
- **Unsuccessful fail-over:** An error occurred when switching user traffic from either the primary to secondary tunnel or the secondary to primary tunnel.


## Supported Standards


Support for the following standards and requests for comments (RFCs) has been added with the Redundant IPSec Tunnel Fail-over functionality:


- RFC 3706, A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers, February 2004

## Redundant IPSec Tunnel Fail-over Configuration

This section provides information and instructions for configuring the Redundant IPSec Tunnel Fail-over feature. These instructions assume that the system was previously configured to support subscriber data sessions either as a core service or an HA.

 **Important:** Parameters configured using this procedure must be configured in the same context on the system.

 **Important:** The system supports a maximum of 32 crypto groups per context. However, configuring crypto groups to use the same loopback interface for secondary IPSec tunnels is not recommended and may compromise redundancy on the chassis.

 **Important:** This section provides the minimum instruction set for configuring crypto groups on the system. For more information on commands that configure additional parameters and options, refer *Command Line Interface Reference*.

To configure the Crypto group to support IPSec:

- Step 1** Configure a crypto group by following the steps in the [Configuring Crypto Group](#) section
- Step 2** Configure one or more ISAKMP policies according to the instructions provided in the [ISAKMP Policy Configuration](#) section of this chapter.
- Step 3** Configure IPSec DPD settings using the instructions provided in the [Dead Peer Detection \(DPD\) Configuration](#) section of this chapter.
- Step 4** Configure an ISAKMP crypto map for the primary and secondary tunnel according to the instructions provided in the [ISAKMP Crypto Map Configuration](#) section of this chapter.
- Step 5** Match the existing ISAKMP crypto map to Crypto group by following the steps in the [Modify ISAKMP Crypto Map Configuration to Match Crypto Group](#) section
- Step 6** Verify your Crypto Group configuration by following the steps in the [Verifying the Crypto Group Configuration](#) section.
- Step 7** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

## Configuring Crypto Group

Use the following example to configure a crypto group on your system for redundant IPSec tunnel fail-over support:

**configure**

**context** <ctxt\_name>

**ikev1 keepalive dpd interval** <dur> **timeout** <dur> **num-retry** <retries>

```

crypto-group <group_name>

    match address <acl_name> [ <preference> ]

    switchover auto [ do-not-revert ]

end

```

Notes:

- <ctxt\_name> is the destination context where the Crypto Group is to be configured.
- <group\_name> is name of the Crypto group you want to configure for IPSec tunnel failover support.
- <acl\_name> is name of the pre-configured crypto ACL. It is used for configurations not implementing the IPSec Tunnel Failover feature and match the crypto map to a previously defined crypto ACL. For more information on crypto ACL, refer [Crypto Access Control List \(ACL\)](#) section of this chapter.

## Modify ISAKMP Crypto Map Configuration to Match Crypto Group

Use the following example to match the crypto group with ISAKMP crypto map on your system:

**configure**

```

context <ctxt_name>

    crypto map <map_name1> ipsec-isakmp

    match crypto-group <group_name> primary

end

```

**configure**

```

context <ctxt_name>

    crypto map <map_name> ipsec-isakmp

    match crypto-group <group_name> secondary

end

```

Notes:

- <ctxt\_name> is the system context in which you wish to create and configure the ISAKMP crypto maps.
- <group\_name> is name of the Crypto group configured in the same context for IPSec Tunnel Failover feature.
- <map\_name1> is name of the preconfigured ISAKMP crypto map to match with crypto group as primary.
- <map\_name2> is name of the preconfigured ISAKMP crypto map to match with crypto group as secondary.

## Verifying the Crypto Group Configuration

These instructions are used to verify the crypto group configuration.

**Step 1** Verify that your system is configured properly with crypto group by entering the following command in Exec Mode in specific context:

```
show crypto group [ summary | name group_name ]
```

The output of this command is a concise listing of crypto group parameter settings configured on the system.

## Dead Peer Detection (DPD) Configuration

This section provides instructions for configuring the Dead Peer Detection (DPD).

Defined by RFC 3706, Dead Peer Detection (DPD) is used to simplify the messaging required to verify communication between peers and tunnel availability.

DPD is configured at the context level and is used in support of the IPsec Tunnel Failover feature (refer to the [Redundant IPsec Tunnel Fail-Over](#) section) and/or to help prevent tunnel state mismatches between an FA and HA when IPsec is used for Mobile IP applications. When used with Mobile IP applications, DPD ensures the availability of tunnels between the FA and HA. (Note that the starIPSECDynTunUp and starIPSECDynTunDown SNMP traps are triggered to indicate tunnel state for the Mobile IP scenario.)

Regardless of the application, DPD must be supported/configured on both security peers. If the system is configured with DPD but it is communicating with a peer that does not have DPD configured, IPsec tunnels still come up. However, the only indication that the remote peer does not support DPD exists in the output of the **show crypto isakmp security-associations summary** command.



**Important:** If DPD is enabled while IPsec tunnels are up, it will not take affect until all of the tunnels are cleared.



**Important:** DPD must be configured in the same context on the system as other IPsec Parameters.

To configure the Crypto group to support IPsec:

- Step 1** Enable dead peer detection on system in support of the IPsec Tunnel Failover feature by following the steps in the [Configuring Crypto Group](#) section
- Step 2** Verify your Crypto Group configuration by following the steps in the [Verifying the DPD Configuration](#) section.
- Step 3** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

## Configuring Crypto Group

Use the following example to configure a crypto group on your system for redundant IPsec tunnel fail-over support:

**configure**

```
context <ctxt_name>

    ikev1 keepalive dpd interval <dur> timeout <dur> num-retry <retries>

end
```

Notes:

- <ctxt\_name> is the destination context where the Crypto Group is to be configured.

## Verifying the DPD Configuration

These instructions are used to verify the dead peer detection configuration.

- Step 1** Verify that your system is configured properly with crypto group with DPD by entering the following command in Exec Mode in specific context:

```
show crypto group [ summary | name group_name ]
```

The output of this command is a concise listing of crypto group parameter settings configured on the system.

## APN Template Configuration to Support L2TP

This section provides instructions for adding L2TP support for APN templates configured on the system.

These instructions assume that the APN template was previously configured on this system.



**Important:** This section provides the minimum instruction set for configuring an APN template to support L2TP for APN. For more information on commands that configure additional parameters and options, refer to the *Command Line Interface Reference*. To configure the APN to support L2TP:

- Step 1** Modify preconfigured APN template by following the steps in the [Modifying APN Template to Support L2TP](#) section
- Step 2** Verify your APN configuration by following the steps in the [Verifying the APN Configuration for L2TP](#) section.
- Step 3** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

### Modifying APN Template to Support L2TP

Use the following example to modify APN template to support L2TP:

**configure**

```

context <ctxt_name>

    apn <apn_name>

        tunnel l2tp [ peer-address <lns_address> [ [ encrypted ] secret <l2tp_secret> ]
[ preference <num> ] [ tunnel-context <tunnel_ctxt_name> ] [ local-address
<agw_ip_address> ] [ crypto-map <map_name> { [ encrypted ] isakmp-secret <crypto_secret>
} ]

    end

```

Notes:

- <ctxt\_name> is the system context in which the APN template is configured.
- <apn\_name> is name of the preconfigured APN template in which you want to configure L2TP support.
- <lns\_address> is IP address of the LNS node to which this APN will communicate.
- <tunnel\_ctxt\_name> is the L2TP context in which the L2TP tunnel is configured.
- <agw\_ip\_address> is the local IP address of the GGSN in which this APN template is configured.
- <map\_name> is the preconfigured crypto map (ISAKMP or manual) which is to use for L2TP.



## Verifying the APN Configuration for L2TP

These instructions are used to verify the APN template configuration for L2TP.

- Step 1** Verify that your APN is configured properly with L2TP by entering the following command in Exec Mode in specific context:

```
show apn { all | name apn_name }
```

The output of this command is a concise listing of FA service parameter settings configured on the system.

# IPsec for LTE/SAE Networks

The Cisco MME (Mobility Management Entity), S-GW (Serving Gateway), and P-GW (Packet Data Network Gateway) support IPsec and IKEv2 encryption using IPv4 and IPv6 addressing in LTE/SAE (Long Term Evolution/System Architecture Evolution) networks. IPsec and IKEv2 encryption enables network domain security for all IP packet-switched networks, providing confidentiality, integrity, authentication, and anti-replay protection via secure IPsec tunnels.

## Encryption Algorithms

IPsec for LTE/SAE supports the following control and data path encryption algorithms:

- AES-CBC-128 (Advanced Encryption Standard-Cipher Block Chaining-128)
- AES-CBC-256 (Advanced Encryption Standard-Cipher Block Chaining-256)
- DES-CBC (Data Encryption Standard-Cipher Block Chaining)
- 3DES-CBC (Triple Data Encryption Standard-Cipher Block Chaining)

## HMAC Functions

IPsec for LTE/SAE supports the following data path HMAC (Hash-based Message Authentication Code) functions:

- AES-XCBC-MAC-96 (Advanced Encryption Standard-X Cipher Block Chaining-Message Authentication Code-96)
- MD5-96 (Message Digest 5-96)
- SHA1-96 (Secure Hash Algorithm 1-96)

IPsec for LTE/SAE supports the following control path HMAC (Hash-based Message Authentication Code) functions:

- AES-XCBC-MAC-96 (Advanced Encryption Standard-X Cipher Block Chaining-Message Authentication Code-96)
- MD5-96 (Message Digest 5-96)
- SHA1-96 (Secure Hash Algorithm 1-96)
- SHA2-256-128 (Secure Hash Algorithm 2-256-128)
- SHA2-384-192 (Secure Hash Algorithm 2-384-192)
- SHA2-512-256 (Secure Hash Algorithm 2-512-256)

## Diffie-Hellman Groups

IPsec for LTE/SAE supports the following Diffie-Hellman groups for IKE and Child SAs (Security Associations):

- Diffie-Hellman Group 1: 768-bit MODP (Modular Exponential) Group
- Diffie-Hellman Group 2: 1024-bit MODP Group

- Diffie-Hellman Group 5: 1536-bit MODP Group
- Diffie-Hellman Group 14: 2048-bit MODP Group
- None: No Diffie-Hellman Group (no perfect forward secrecy)

## Dynamic Node-to-Node IPSec Tunnels

IPSec for LTE/SAE enables network nodes to initiate an IPSec tunnel with another node for secure signaling and data traffic between the nodes, enabling up to 64K dynamic, service-integrated IPSec tunnels per chassis. Once established, a dynamic node-to-node IPSec tunnel continues to carry all of the signaling and/or bearer traffic between the nodes. Dynamic node-to-node IPSec for LTE/SAE is supported on the S1-MME interface for signaling traffic between the eNodeB and the MME, on the S1-U interface for data traffic between the eNodeB and the S-GW, and on the S5 interface for data traffic between the S-GW and the P-GW.

Dynamic node-to-node IPSec gets configured using dynamic IKEv2 crypto templates, which are used to specify common cryptographic parameters for the IPSec tunnels such as the encryption algorithm, HMAC function, and Diffie-Hellman group. Additional information necessary for creating node-to-node IPSec tunnels such as revocation lists are fetched dynamically from the IPSec tunnel requests.

For configuration instructions for dynamic node-to-node IPSec, see the configuration chapter in the administration guides for the MME, S-GW, and P-GW.

## ACL-based Node-to-Node IPSec Tunnels

Node-to-node IPSec for LTE/SAE can also be configured using crypto ACLs (Access Control Lists), which define the matching criteria used for routing subscriber data packets over an IPSec tunnel. ACL-based node-to-node IPSec tunnels are supported on the S1-MME interface for signaling traffic between the eNodeB and the MME, on the S1-U interface for data traffic between the eNodeB and the S-GW, and on the S5 interface for data traffic between the S-GW and the P-GW.

Unlike other ACLs that are applied to interfaces, contexts, or to one or more subscribers, crypto ACLs are applied via matching criteria to crypto maps, which define tunnel policies that determine how IPSec is implemented for subscriber data packets. Prior to routing, the system examines the properties of each subscriber data packet. If the packet properties match the criteria specified in the crypto ACL, the system initiates the IPSec policy dictated by the crypto map. ACL-based node-to-node IPSec tunnels are configured using either IKEv2-IPv4 or IKEv2-IPv6 crypto maps for IPv4 or IPv6 addressing.

Up to 150 ACL-based node-to-node IPSec tunnels are supported on the system, each with one SA bundle that includes one Tx and one Rx endpoint. However, to avoid significant performance degradation, dynamic node-to-node IPSec tunnels are recommended. If ACL-based node-to-node IPSec tunnels are used, a limit of about ten ACL-based node-to-node IPSec tunnels per system is recommended.

For configuration instructions for ACL-based node-to-node IPSec, see the configuration chapter in the administration guides for the MME, S-GW, and P-GW.

For more information on ACLs, see the *System Administration Guide*.

## Traffic Selectors

Per RFC 4306, when a packet arrives at an IPSec subsystem and matches a 'protect' selector in its Security Policy Database (SPD), the subsystem must protect the packet via IPSec tunneling. Traffic selectors enable an IPSec subsystem to accomplish this by allowing two endpoints to share information from their SPDs. Traffic selector payloads contain

the selection criteria for packets being sent over IPSec security associations (SAs). Traffic selectors can be created on the P-GW, S-GW, and MME for dynamic node-to-node IPSec tunnels during crypto template configuration by specifying a range of peer IPv4 or IPV6 addresses from which to carry traffic over IPSec tunnels.

For example, consider an eNodeB with an IP address of 1.1.1.1 and an S-GW with a service address of 2.2.2.2. The S-GW is registered to listen for IKE requests from the eNodeBs in the network using the following information:

- Local Address: 2.2.2.2
- Peer Address Network: 1.1.0.0 Mask: 255.255.0.0
- Payload ACL (Access Control List): udp host 2.2.2.2 eq 2123 1.1.0.0 0.0.255.255

When an IKE request arrives the S-GW from eNodeB address 1.1.1.1, the IPSec subsystem converts the payload ACL to: udp host 2.2.2.2 eq 2123 host 1.1.1.1, and this payload becomes the traffic selector for the IPSec tunnel being negotiated.

To properly accommodate control traffic between IPSec nodes, each child SA must include at least two traffic selectors: one with a well-known port in the source address, and one with a well-known port in the destination address. Continuing the example above, the final traffic selectors would be:

- Destination port as well-known port: udp host 2.2.2.2 1.1.0.0 0.0.255.255 eq 2123
- Source port as well-known port: udp host 2.2.2.2 eq 2123 1.1.0.0 0.0.255.255

Note that for ACL-based node-to-node IPSec tunnels, the configured crypto ACL becomes the traffic selector with no modification.

## Authentication Methods

IPSec for LTE/SAE includes the following authentication methods:

- **PSK (Pre-Shared Key) Authentication:** A pre-shared key is a shared secret that was previously shared between two network nodes. IPSec for LTE/SAE supports PSK such that both IPSec nodes must be configured to use the same shared secret.
- **X.509 Certificate-based Peer Authentication:** IPSec for LTE/SAE supports X.509 certificate-based peer authentication and CA (Certificate Authority) certificate authentication as described below.

## X.509 Certificate-based Peer Authentication

X.509 specifies standard formats for public key certificates, certificate revocation lists, attribute certificates, and a certification path validation algorithm. X.509 certificates are configured on each IPSec node so that it can send the certificate as part of its IKE\_AUTH\_REQ for the remote node to authenticate it. These certificates can be in PEM (Privacy Enhanced Mail) or DER (Distinguished Encoding Rules) format, and can be fetched from a repository via HTTP or FTP.

CA certificate authentication is used to validate the certificate that the local node receives from a remote node during an IKE\_AUTH exchange.

A maximum of sixteen certificates and sixteen CA certificates are supported per system. One certificate is supported per service, and a maximum of four CA certificates can be bound to one crypto template.

For configuration instructions for X.509 certificate-based peer authentication, see the configuration chapter in the administration guides for the MME, S-GW, and P-GW.

The figure below shows the message flow during X.509 certificate-based peer authentication. The table that follows the figure describes each step in the message flow.

Figure 58. X.509 Certificate-based Peer Authentication

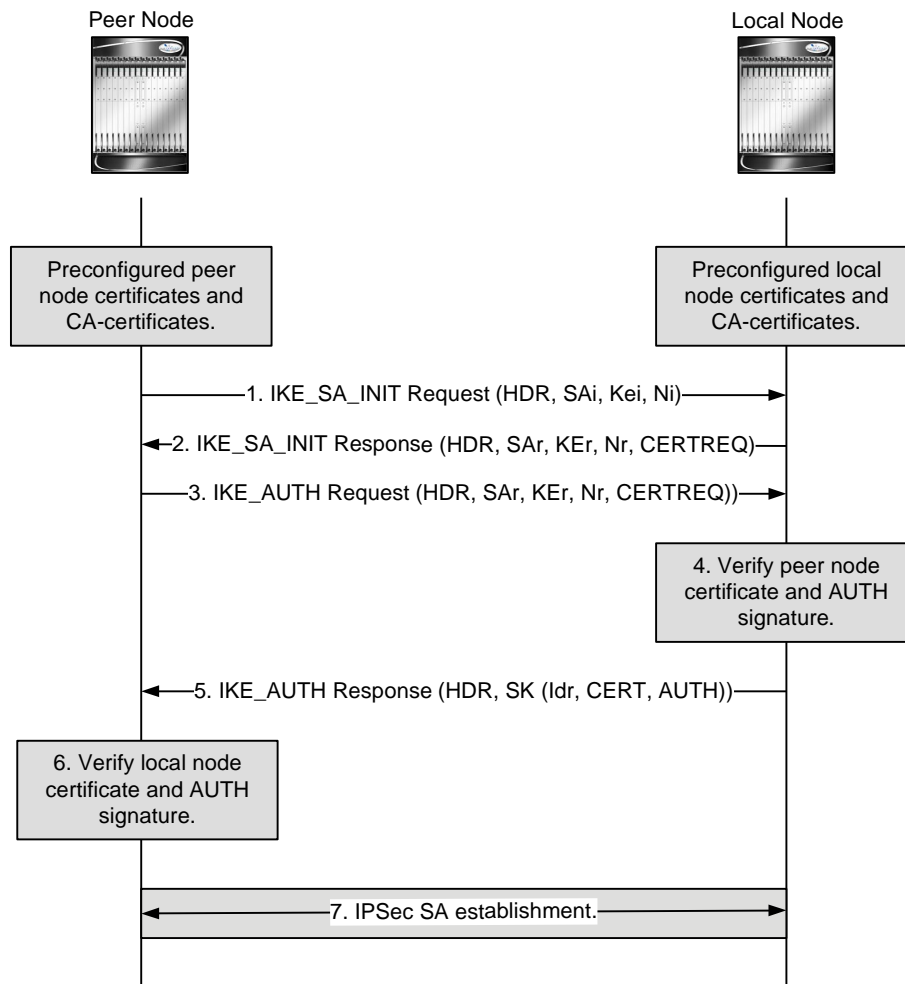


Table 30. X.509 Certificate-based Peer Authentication

Step	Description
1.	The peer node initiates an IKEv2 exchange with the local node, known as the IKE_SA_INIT exchange, by issuing an IKE_SA_INIT Request to negotiate cryptographic algorithms, exchange nonces, and perform a Diffie-Hellman exchange with the local node.
2.	The local node responds with an IKE_SA_INIT Response by choosing a cryptographic suite from the initiator's offered choices, completing the Diffie-Hellman and nonce exchanges with the peer node. In addition, the local node includes the list of CA certificates that it will accept in its CERTREQ payload. For successful peer authentication, the CERTREQ payload must contain at least one CA certificate that is in the trust chain of the peer certificate. At this point in the negotiation, the IKE_SA_INIT exchange is complete and all but the headers of all the messages that follow are encrypted and integrity-protected.

Step	Description
3.	The peer node initiates an IKE_AUTH exchange with the local node by including the IDi payload, setting the CERT payload to the peer certificate, and including the AUTH payload containing the signature of the previous IKE_SA_INIT Request message (in step 1) generated using the private key of the peer certificate. The authentication algorithm used to generate the AUTH payload is also included in the AUTH payload. The peer node also includes the CERTREQ payload containing the list of SHA-1 hash algorithms for local node authentication. For successful server authentication, the CERTREQ payload must contain at least one CA certificate that is in the trust chain of the peer certificate.
4.	Using the CA certificate corresponding to the peer certificate, the local node first verifies that the peer certificate in the CERT payload has not been modified and the identity included in the IDi corresponds to the identity in the peer certificate. If the verification is successful, using the public key of the peer certificate, the local node generates the expected AUTH payload and compares it with the received AUTH payload. If they match, the authentication of the peer node is successful. Otherwise, the local node sends an IKEv2 Notification message indicating authentication failure.
5.	The local node responds with the IKE_AUTH Response, including the IDr payload, setting the CERT payload to the local node certificate, and including the AUTH payload containing the signature of the IKE_SA_INIT Response message (in step 2) generated using the private key of the local node certificate. The authentication algorithm used to generate the AUTH payload is also included in the AUTH payload.
6.	Using the CA certificate corresponding to the local node certificate, the peer node first verifies that the local node certificate in the CERT payload has not been modified. If the verification is successful, using the public key of the local node certificate, the peer generates the expected AUTH payload and compares it with the received AUTH payload. If they match, the local node authentication is successful. This completes the IKE_AUTH exchange.
7.	An IPSec SA gets established between the peer node and the local node. If more IPSec SAs are needed, either the peer or local node can initiate the creation of additional Child SAs using a CREATE_CHILD_SA exchange.

## Certificate Revocation Lists

Certificate revocation lists track certificates that have been revoked by the CA (Certificate Authority) and are no longer valid. Per RFC 3280, during certificate validation, IPSec for LTE/SAE checks the certificate revocation list to verify that the certificate the local node receives from the remote node has not expired and hence is still valid.

During configuration via the system CLI, one certificate revocation list is bound to each crypto template and can be fetched from its repository via HTTP or FTP.

## Child SA Rekey Support

Rekeying of an IKEv2 Child Security Association (SA) occurs for an already established Child SA whose lifetime (either time-based or data-based) is about to exceed a maximum limit. The IPSec subsystem initiates rekeying to replace the existing Child SA. During rekeying, two Child SAs exist momentarily (500ms or less) to ensure that transient packets from the original Child SA are processed by the IPSec node and not dropped.

Child SA rekeying is disabled by default, and rekey requests are ignored. This feature gets enabled in the Crypto Configuration Payload Mode of the system's CLI.

## IKEv2 Keep-Alive Messages (Dead Peer Detection)

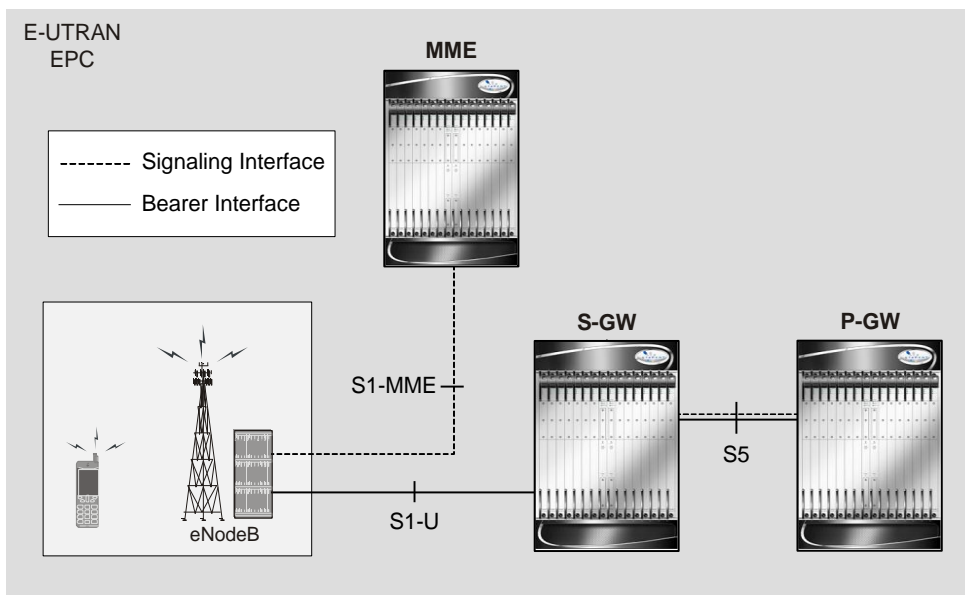
IPSec for LTE/SAE supports IKEv2 keep-alive messages, also known as Dead Peer Detection (DPD), originating from both ends of an IPSec tunnel. Per RFC 3706, DPD is used to simplify the messaging required to verify communication

between peers and tunnel availability. You configure DPD on each IPSec node. You can also disable DPD, and the node will not initiate DPD exchanges with other nodes. However, the node always responds to DPD availability checks initiated by another node regardless of its DPD configuration.

## E-UTRAN/EPC Logical Network Interfaces Supporting IPSec Tunnels

The figure below shows the logical network interfaces over which secure IPSec tunnels can be created in an E-UTRAN/EPC (Evolved UMTS Terrestrial Radio Access Network/Evolved Packet Core) network. The table that follows the figure provides a description of each logical network interface.

**Figure 59. E-UTRAN/EPC Logical Network Interfaces Supporting IPSec Tunnels**



**Table 31. E-UTRAN/EPC Logical Network Interfaces Supporting IPSec Tunnels**

Interface	Description
-----------	-------------

Interface	Description
S1-MME Interface	<p>This interface is the reference point for the control plane protocol between the eNodeB and the MME. The S1-MME interface uses S1-AP (S1- Application Protocol) over SCTP (Stream Control Transmission Protocol) as the transport layer protocol for guaranteed delivery of signaling messages between the MME and the eNodeB (S1). When configured, the S1-AP over SCTP signaling traffic gets carried over an IPsec tunnel.</p> <p>When a subscriber UE initiates a connection with the eNodeB, the eNodeB initiates an IPsec tunnel with the MME, and SCTP signaling for all subsequent subscriber UEs served by this MME gets carried over the same IPsec tunnel. The MME can also initiate an IPsec tunnel with the eNodeB when the following conditions exist:</p> <ul style="list-style-type: none"> <li>• The first tunnel setup is always triggered by the eNodeB. This is the tunnel over which initial SCTP exchanges occur.</li> <li>• The MME initiates additional tunnels to the eNodeB after an SCTP connection is set up if the MME is multi-homed: a tunnel is initiated from MME's second address to the eNodeB.</li> <li>• The eNodeB is multi-homed: tunnels are initiated from the MME's primary address to each secondary address of the eNodeB.</li> <li>• Both of the prior two conditions: a tunnel is initiated from each of MME's addresses to each address of the eNodeB.</li> </ul>
S1-U Interface	<p>This interface is the reference point for bearer channel tunneling between the eNodeB and the S-GW. Typically, the eNodeB initiates an IPsec tunnel with the S-GW over this interface for subscriber data traffic. But the S-GW may also initiate an IPsec tunnel with the eNodeB, if required.</p>
S5 Interface	<p>This interface is the reference point for tunneling between the S-GW and the P-GW. Based on the requested APN from a subscriber UE, the MME selects both the S-GW and the P-GW that the S-GW connects to. GTP-U data traffic is carried over the IPsec tunnel between the S-GW and P-GW for the current and all subsequent subscriber UEs.</p>

## IPsec Tunnel Termination

IPsec tunnel termination occurs during the following scenarios:

- **Idle Tunnel Termination:** When a session manager for a service detects that all subscriber sessions using a given IPsec tunnel have terminated, the IPsec tunnel also gets terminated after a timeout period.
- **Service Termination:** When a service running on a network node is brought down for any reason, all corresponding IPsec tunnels get terminated. This may be caused by the interface for a service going down, a service being stopped manually, or a task handling an IPsec tunnel restarting.
- **Unreachable Peer:** If a network node detects an unreachable peer via Dead Peer Detection (DPD), the IPsec tunnel between the nodes gets terminated. DPD can be enabled per P-GW, S-GW, and MME service via the system CLI during crypto template configuration.
- **E-UTRAN Handover Handling:** Any IPsec tunnel that becomes unusable due to an E-UTRAN network handover gets terminated, while the network node to which the session is handed initiates a new IPsec tunnel for the session.



# Appendix I

## L2TP Access Concentrator

---

This chapter describes the Layer 2 Tunneling Protocol (L2TP) Access Concentrator (LAC) functionality support on Cisco® ASR 5x00 chassis and explains how it is configured.

The product Administration Guides provide examples and procedures for configuration of basic services on the system. It is recommended that you select the configuration example that best meets your service model, and configure the required elements for that model, as described in the respective product Administration Guide, before using the procedures in this chapter.



**Important:** The L2TP Access Concentrator is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

---

When enabled through the session license and feature use key, the system supports L2TP for encapsulation of data packets between it and one or more L2TP Network Server (LNS) nodes. In the system, this optional packet encapsulation, or tunneling, is performed by configuring L2TP Access Concentrator (LAC) services within contexts.



**Important:** The LAC service uses UDP ports 13660 through 13668 as the source port for sending packets to the LNS.

---

## Applicable Products and Relevant Sections

The LAC feature is supported for various products. The following table indicates the products on which the feature is supported and the relevant sections within the chapter that pertain to that product.

Applicable Product(s)	Refer to Sections
PDSN/FA/HA	<ul style="list-style-type: none"> <li>• <i>Supported LAC Service Configurations for PDSN Simple IP</i></li> <li>• <i>Supported LAC Service Configuration for Mobile IP</i></li> <li>• <i>Configuring Subscriber Profiles for L2TP Support</i> <ul style="list-style-type: none"> <li>• <i>RADIUS and Subscriber Profile Attributes Used</i></li> <li>• <i>Configuring Local Subscriber Profiles for L2TP Support</i></li> <li>• <i>Tunneling All Subscribers in a Specific Context Without Using RADIUS Attributes</i></li> </ul> </li> <li>• <i>Configuring LAC Services</i></li> <li>• <i>Modifying PDSN Services for L2TP Support</i></li> </ul>
GGSN/SGSN/FA/P-GW	<ul style="list-style-type: none"> <li>• <i>Supported LAC Service Configurations for the GGSN</i></li> <li>• <i>Supported LAC Service Configuration for Mobile IP</i></li> <li>• <i>Configuring Subscriber Profiles for L2TP Support</i> <ul style="list-style-type: none"> <li>• <i>RADIUS and Subscriber Profile Attributes Used</i></li> <li>• <i>Configuring Local Subscriber Profiles for L2TP Support</i></li> </ul> </li> <li>• <i>Configuring LAC Services</i></li> <li>• <i>Modifying APN Templates to Support L2TP</i></li> </ul>
ASN GW	<ul style="list-style-type: none"> <li>• <i>Supported LAC Service Configuration for Mobile IP</i></li> <li>• <i>Configuring Subscriber Profiles for L2TP Support</i> <ul style="list-style-type: none"> <li>• <i>RADIUS and Subscriber Profile Attributes Used</i></li> <li>• <i>Configuring Local Subscriber Profiles for L2TP Support</i></li> <li>• <i>Tunneling All Subscribers in a Specific Context Without Using RADIUS Attributes</i></li> </ul> </li> <li>• <i>Configuring LAC Services</i></li> </ul>

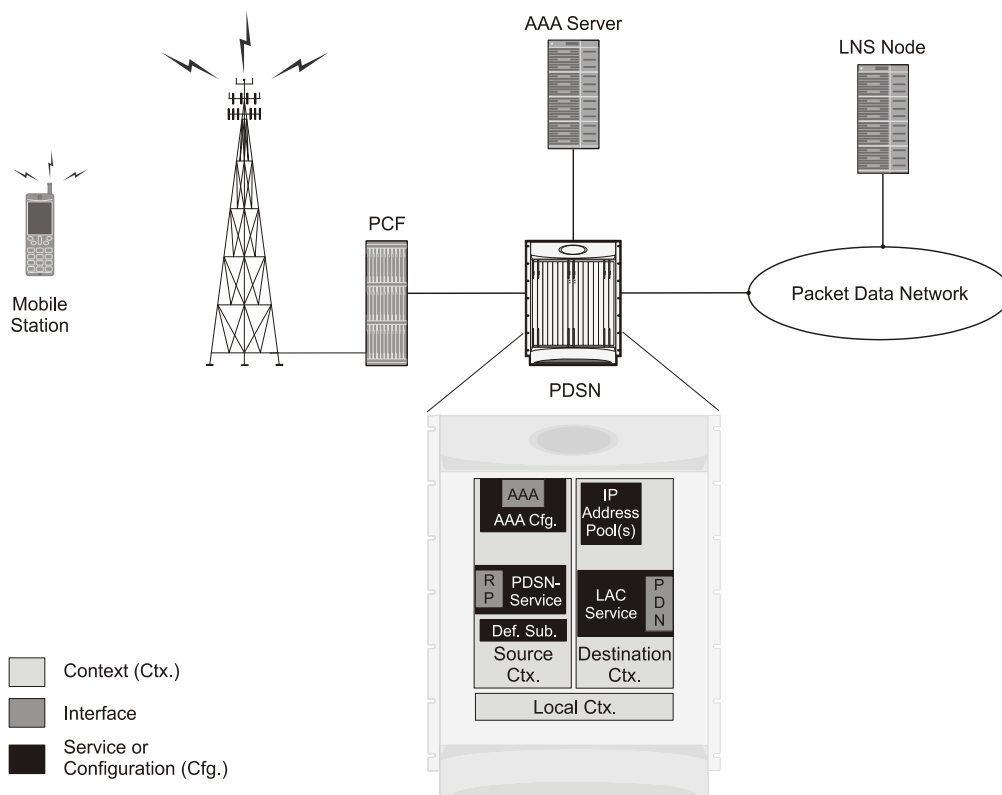
## Supported LAC Service Configurations for PDSN Simple IP

LAC services can be applied to incoming PPP sessions using one of the following methods:

- **Attribute-based tunneling:** This method is used to encapsulate PPP packets for only specific users, identified during authentication. In this method, the LAC service parameters and allowed LNS nodes that may be communicated with are controlled by the user profile for the particular subscriber. The user profile can be configured locally on the system or remotely on a RADIUS server.
- **PDSN Service-based compulsory tunneling:** This method of tunneling is used to encapsulate all incoming PPP traffic from the R-P interface coming into a PDSN service, and tunnel it to an LNS peer for authentication. It should be noted that this method does not consider subscriber configurations, since all authentication is performed by the peer LNS.

Each LAC service is bound to a single system interface configured within the same system context. It is recommended that this context be a destination context as displayed in the following figure.

Figure 60. LAC Service Configuration for SIP



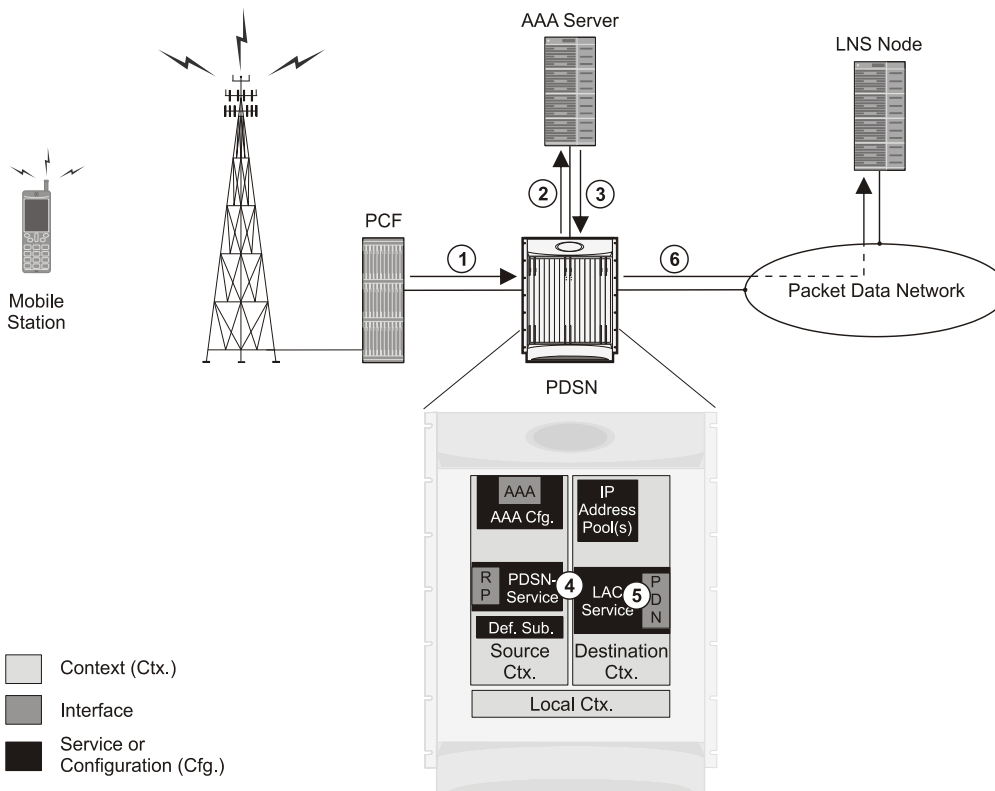
## Attribute-based Tunneling

This section describes the working of attribute-based tunneling and its configuration.

## How The Attribute-based L2TP Configuration Works

The following figure and the text that follows describe how Attribute-based tunneling is performed using the system.

**Figure 61. Attribute-based L2TP Session Processing for SIP**



1. A subscriber session from the PCF is received by the PDSN service over the R-P interface.
2. The PDSN service attempts to authenticate the subscriber. The subscriber could be configured either locally or remotely on a RADIUS server. Figure above shows subscriber authentication using a RADIUS AAA server.
3. The RADIUS server returns an Access-Accept message, which includes attributes indicating that session data is to be tunneled using L2TP, and the name and location of the LAC service to use. An attribute could also be provided indicating the LNS peer to connect to.
4. The PDSN service receives the information and then forwards the packets to the LAC service, configured within the Destination context.
5. The LAC service, upon receiving the packets, encapsulates the information and forwards it to the appropriate PDN interface for delivery to the LNS.
6. The encapsulated packets are sent to the peer LNS through the packet data network where they will be un-encapsulated.

## Configuring Attribute-based L2TP Support for PDSN Simple IP

This section provides a list of the steps required to configure attribute-based L2TP support for use with PDSN Simple IP applications. Each step listed refers to a different section containing the specific instructions for completing the required procedure.



**Important:** These instructions assume that the system was previously configured to support subscriber data sessions as a PDSN.

- Step 1** Configure the subscriber profiles according to the information and instructions located in the *Configuring Subscriber Profiles for L2TP Support* section of this chapter.
- Step 2** Configure one or more LAC services according to the information and instructions located in the *Configuring LAC Services* section of this chapter.
- Step 3** Configure the PDSN service(s) with the tunnel context location according to the instructions located in the *Modifying PDSN Services for L2TP Support* section of this chapter.
- Step 4** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

## PDSN Service-based Compulsory Tunneling

This section describes the working of service-based compulsory tunneling and its configuration.

### How PDSN Service-based Compulsory Tunneling Works

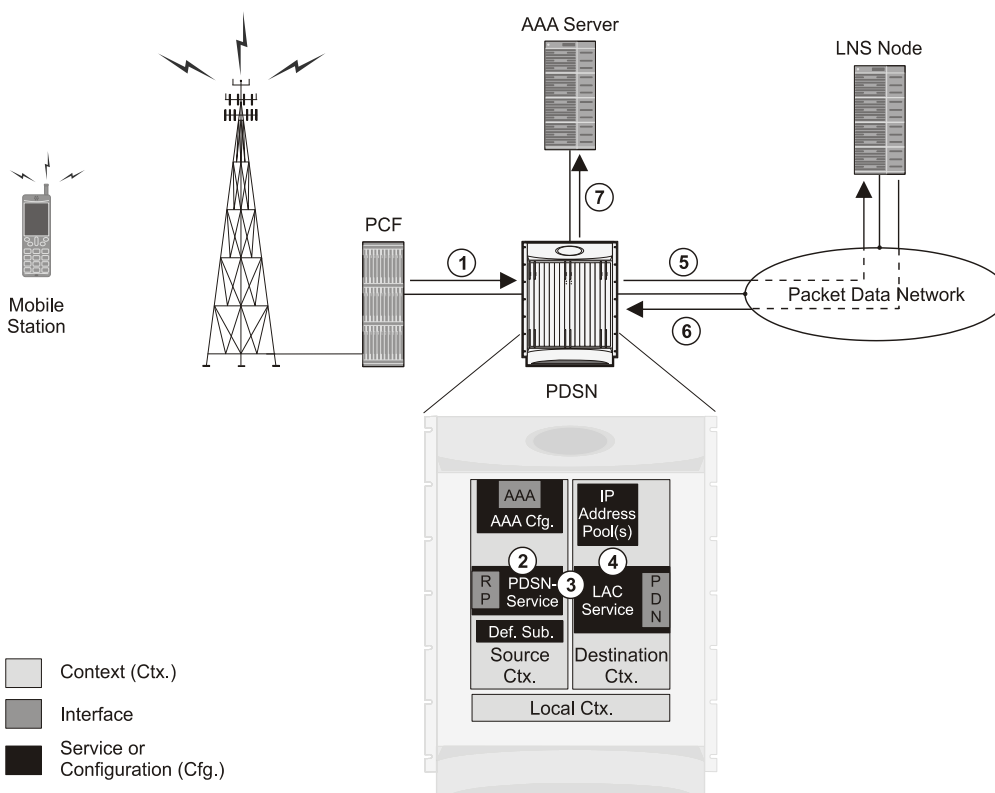
PDSN Service-based compulsory tunneling enables wireless operators to send all PPP traffic to remote LNS peers over an L2TP tunnel for authentication. This means that no PPP authentication is performed by the system.

Accounting start and interim accounting records are still sent to the local RADIUS server configured in the system's AAA Service configuration. When the L2TP session setup is complete, the system starts its call counters and signals the RADIUS server to begin accounting. The subscriber name for accounting records is based on the NAI-constructed name created for each session.

PDSN service-based compulsory tunneling requires the modification of one or more PDSN services and the configuration of one or more LAC services.

The following figure and the text that follows describe how PDSN service-based compulsory tunneling is performed using the system.

Figure 62. PDSN Service-based Compulsory Tunneling Session Processing



1. A subscriber session from the PCF is received by the PDSN service over the R-P interface.
  2. The PDSN service detects its **tunnel-type** parameter is configured to L2TP and its **tunnel-context** parameter is configured to the Destination context.
  3. The PDSN forwards all packets for the session to a LAC service configured in the Destination context. If multiple LAC services are configured, session traffic will be routed to each using a round-robin algorithm.
  4. The LAC service initiates an L2TP tunnel to one of the LNS peers listed as part of its configuration.
  5. Session packets are passed to the LNS over a packet data network for authentication.
  6. The LNS authenticates the session and returns an Access-Accept to the PDSN.
  7. The PDSN service initiates accounting for the session using a constructed NAI.
- Session data traffic is passed over the L2TP tunnel established in step 4.

## Configuring L2TP Compulsory Tunneling Support for PDSN Simple IP

This section provides a list of the steps required to configure L2TP compulsory tunneling support for use with PDSN Simple IP applications. Each step listed refers to a different section containing the specific instructions for completing the required procedure.



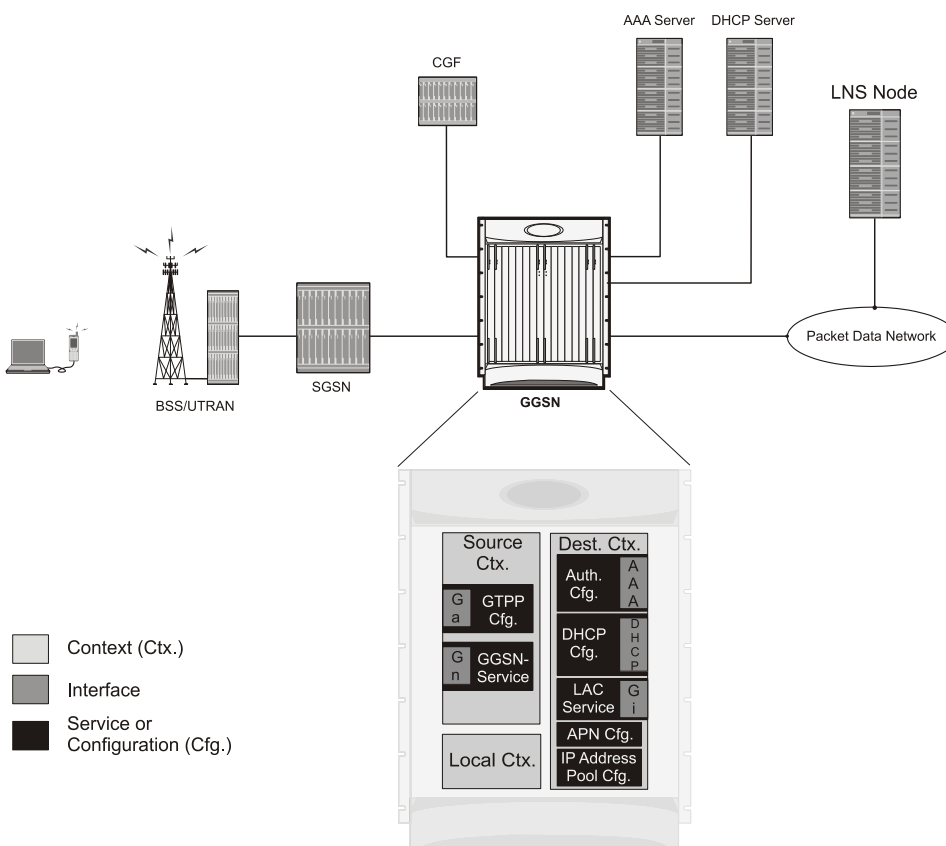
**Important:** These instructions assume that the system was previously configured to support subscriber data sessions as a PDSN.

- Step 1** Configure one or more LAC services according to the information and instructions located in the *Configuring LAC Services* section of this chapter.
- Step 2** Configure the PDSN service(s) according to the instructions located in the *Modifying PDSN Services for L2TP Support* section of this chapter.
- Step 3** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

## Supported LAC Service Configurations for the GGSN and P-GW

As mentioned previously, L2TP is supported through the configuration of LAC services on the system. Each LAC service is bound to a single system interface configured within the same system destination context as displayed in following figure.

Figure 63. GGSN LAC Service Configuration



LAC services are applied to incoming subscriber PDP contexts based on the configuration of attributes either in the GGSN's Access Point Name (APN) templates or in the subscriber's profile. Subscriber profiles can be configured locally on the system or remotely on a RADIUS server.

LAC service also supports domain-based L2TP tunneling with LNS. This method is used to create multiple tunnels between LAC and LNS on the basis of values received in "Tunnel-Client-Auth-ID" or "Tunnel-Server-Auth-ID" attribute received from AAA Server in Access-Accept as a key for tunnel selection and creation. When the LAC needs to establish a new L2TP session, it first checks if there is any existing L2TP tunnel with the peer LNS based on the value of key "Tunnel-Client-Auth-ID" or "Tunnel-Server-Auth-ID" attribute. If no such tunnel exists for the key, it will create a new Tunnel with the LNS.

If LAC service needs to establish a new tunnel for new L2TP session with LNS and the tunnel create request fails because maximum tunnel creation limit is reached, LAC will try other LNS addresses received from AAA server in Access-Accept message. If all available peer-LNS are exhausted, LAC service will reject the call



L2TP tunnel parameters are configured within the APN template and are applied to all subscribers accessing the APN. However, L2TP operation will differ depending on the subscriber's PDP context type as described below:

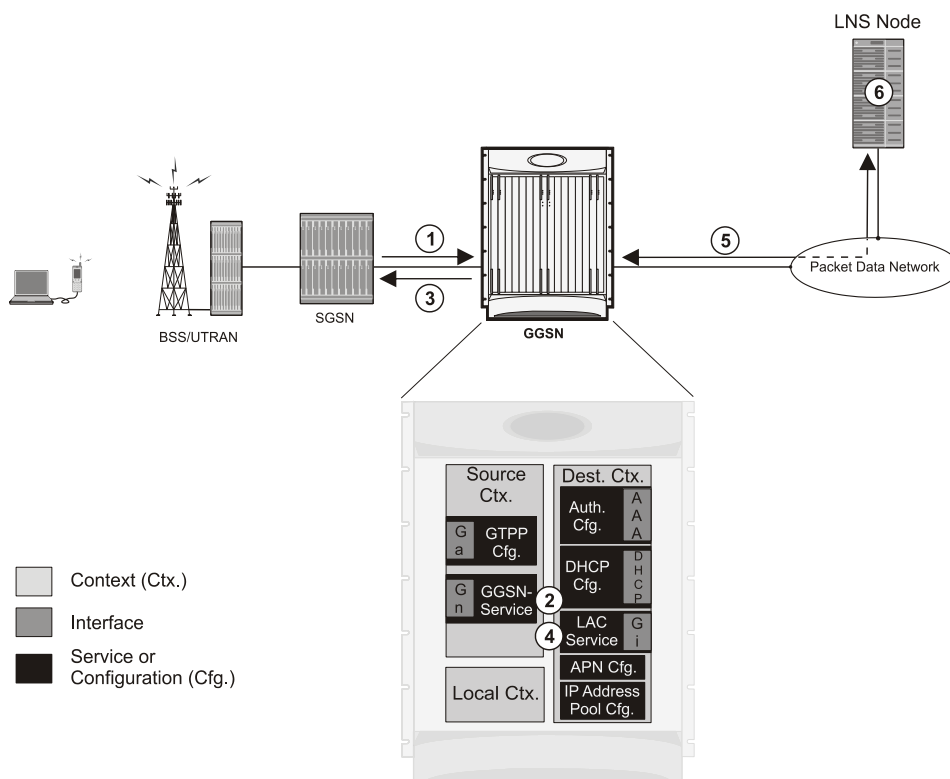
- **Transparent IP:** The APN template's L2TP parameter settings will be applied to the session.
- **Non-transparent IP:** Since authentication is required, L2TP parameter attributes in the subscriber profile (if configured) will take precedence over the settings in the APN template.
- **PPP:** The APN template's L2TP parameter settings will be applied and all of the subscriber's PPP packets will be forwarded to the specified LNS.

More detailed information is located in the sections that follow.

## Transparent IP PDP Context Processing with L2TP Support

The following figure and the text that follows describe how transparent IP PDP contexts are processed when L2TP tunneling is enabled.

**Figure 64. Transparent IP PDP Context Call Processing with L2TP Tunneling**



1. A Create PDP Context Request message for a subscriber session is sent from the SGSN to the GGSN service over the Gn interface. The message contains information such as the PDP Type, APN, and charging characteristics.
2. The GGSN determines whether or not it is configured with an APN identical to the one specified in the message. If so, it determines how to process the session based on the configuration of the APN.

The APN configuration indicates such things as the IP address of the LNS, the system destination context in which a LAC service is configured, and the outbound username and password that will be used by the LNS to authenticate incoming

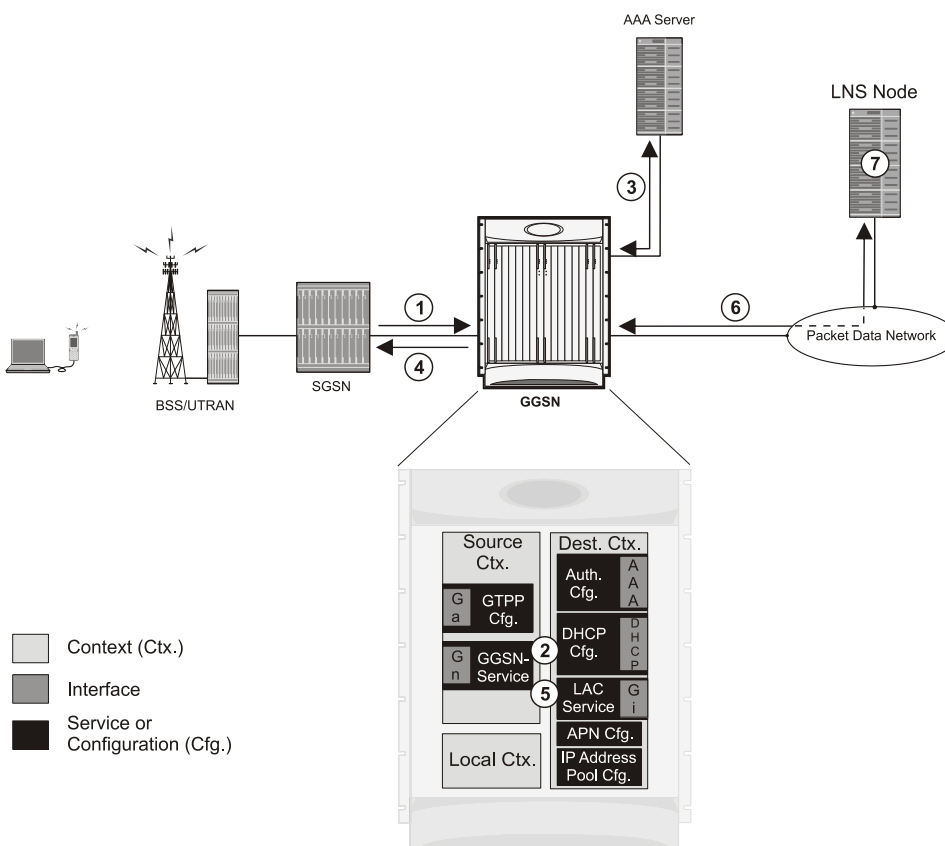
sessions. If no outbound information is configured, the subscriber's International Mobile Subscriber Identity (IMSI) is used as the username at the peer LNS.

1. The GGSN returns an affirmative Create PDP Context Response to the SGSN over the Gn interface.
2. The GGSN passes data received from the MS to a LAC service.
3. The LAC service encapsulates the IP packets and forwards it to the appropriate Gi interface for delivery to the LNS.
4. The LNS un-encapsulates the packets and processes them as needed. The processing includes IP address allocation.

## Non-transparent IP PDP Context Processing with L2TP Support

The following figure and the text that follows describe how non-transparent IP PDP contexts are processed when L2TP tunneling is enabled.

**Figure 65. Non-transparent IP PDP Context Call Processing with L2TP Tunneling**



1. A Create PDP Context Request message for a subscriber session is sent from the SGSN to the GGSN service over the Gn interface. The message contains information such as the PDP Type, APN, and charging characteristics.
2. The GGSN determines whether or not it is configured with an APN identical to the one specified in the message. If so, it determines how to process the session based on the configuration of the APN.

The APN configuration indicates such things as the IP address of the LNS, the system destination context in which a LAC service is configured, and the outbound username and password that will be used by the LNS to authenticate incoming sessions. If no outbound information is configured, the subscriber's username is sent to the peer LNS.

3. The GGSN service authenticates the subscriber. The subscriber could be configured either locally or remotely on a RADIUS server. Figure above shows subscriber authentication using a RADIUS AAA server. As part of the authentication, the RADIUS server returns an Access-Accept message.

The message may include attributes indicating that session data is to be tunneled using L2TP, and the name and location of the LAC service to use. An attribute could also be provided indicating the LNS peer to connect to.

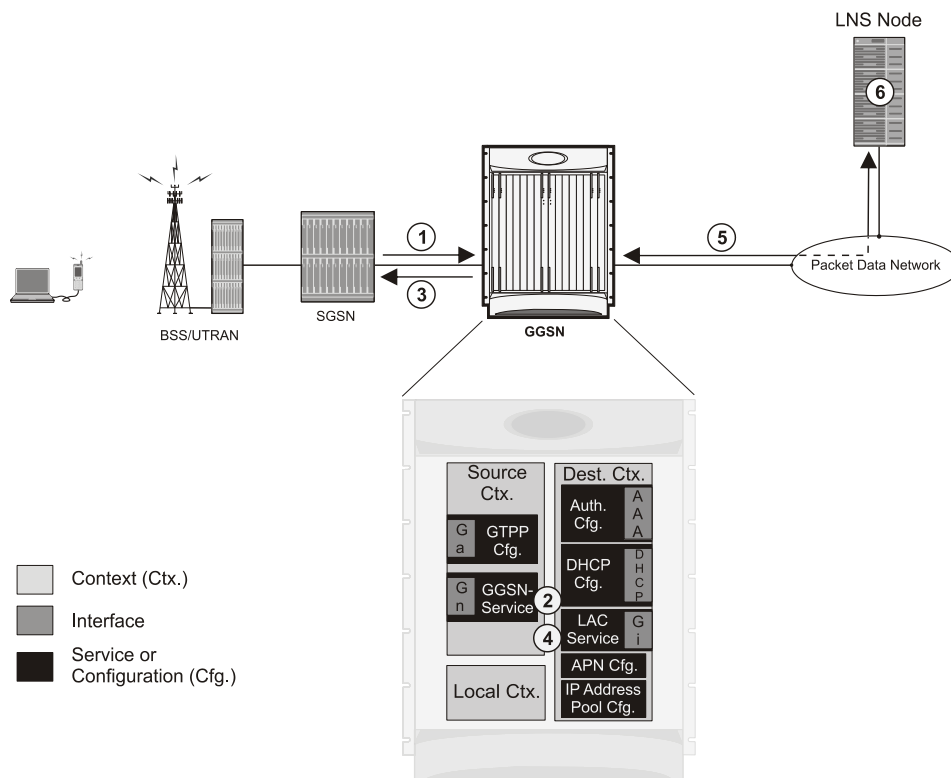
If these attributes are supplied, they take precedence over those specified in the APN template.

4. The GGSN returns an affirmative Create PDP Context Response to the SGSN over the Gn interface.
5. The GGSN passes data received from the MS to a LAC service.
6. The LAC service encapsulates the IP packets and forwards it to the appropriate Gi interface for delivery to the LNS.
7. The LNS un-encapsulates the packets and processes them as needed. The processing includes authentication and IP address allocation.

## PPP PDP Context Processing with L2TP Support

The following figure and the text that follows describe how non-transparent IP PDP contexts are processed when L2TP tunneling is enabled.

Figure 66. PPP PDP Context Call Processing with L2TP Tunneling



1. A Create PDP Context Request message for a subscriber session is sent from the SGSN to the GGSN service over the Gn interface. The message contains information such as the PDP Type, APN, and charging characteristics.
2. The GGSN determines whether or not it is configured with an APN identical to the one specified in the message. If so, it determines how to process the session based on the configuration of the APN. The APN configuration indicates such things as the IP address of the LNS, the system destination context in which a LAC service is configured.  
  
Note that L2TP support could also be configured in the subscriber's profile. If the APN is not configured for L2TP tunneling, the system will attempt to authenticate the subscriber. The tunneling parameters in the subscriber's profile would then be used to determine the peer LNS.
3. The GGSN returns an affirmative Create PDP Context Response to the SGSN over the Gn interface.
4. The GGSN passes the PPP packets received from the MS to a LAC service.
5. The LAC service encapsulates the PPP packets and forwards it to the appropriate Gi interface for delivery to the LNS.
6. The LNS un-encapsulates the packets and processes them as needed. The processing includes PPP termination, authentication (using the username/password provided by the subscriber), and IP address allocation.

## Configuring the GGSN or P-GW to Support L2TP

This section provides a list of the steps required to configure the GGSN or P-GW to support L2TP. Each step listed refers to a different section containing the specific instructions for completing the required procedure.



**Important:** These instructions assume that the system was previously configured to support subscriber data sessions as a GGSN or P-GW.

1. Configure the APN template to support L2TP tunneling according to the information and instructions located in the *Modifying APN Templates to Support L2TP* section of this chapter.



**Important:** L2TP tunneling can be configured within individual subscriber profiles as opposed/or in addition to configuring support with an APN template. Subscriber profile configuration is described in the *Configuring Subscriber Profiles for L2TP Support* section of this chapter.

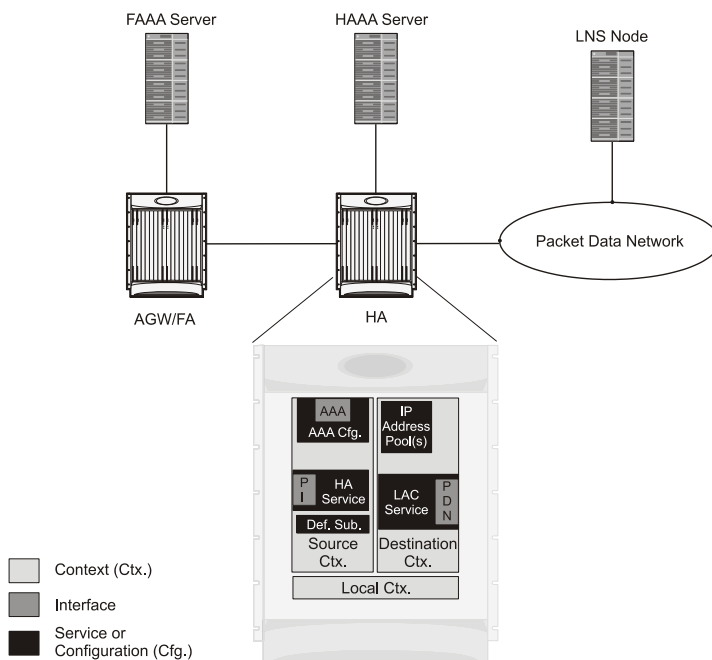
2. Configure one or more LAC services according to the information and instructions located in the *Configuring LAC Services* section of this chapter.
3. Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

## Supported LAC Service Configuration for Mobile IP

LAC services can be applied to incoming MIP sessions using attribute-based tunneling. Attribute-based tunneling is used to encapsulate PPP packets for specific users, identified during authentication. In this method, the LAC service parameters and allowed LNS nodes that may be communicated with are controlled by the user profile for the particular subscriber. The user profile can be configured locally on the system or remotely on a RADIUS server.

Each LAC service is bound to a single system interface within the same system context. It is recommended that this context be a destination context as displayed in figure below.

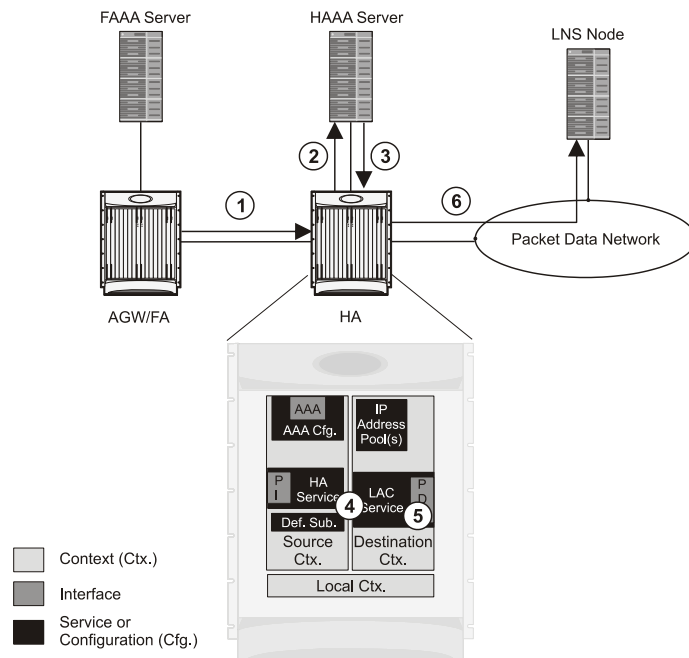
Figure 67. LAC Service Configuration for MIP



## How The Attribute-based L2TP Configuration for MIP Works

The following figure and the text that follows describe how Attribute-based tunneling for MIP is performed using the system.

Figure 68. Attribute-based L2TP Session Processing for MIP



1. A subscriber session from the FA is received by the HA service over the Pi interface.
2. The HA service attempts to authenticate the subscriber. The subscriber could be configured either locally or remotely on a RADIUS server. Figure above shows subscriber authentication using a RADIUS AAA server.
3. The RADIUS server returns an Access-Accept message, which includes attributes indicating that session data is to be tunneled using L2TP, and the name and location of the LAC service to use. An attribute could also be provided indicating the LNS peer to connect to.
4. The HA service receives the information and then forwards the packets to the LAC service, configured within the Destination context.
5. The LAC service, upon receiving the packets, encapsulates the information and forwards it to the appropriate PDN interface for delivery to the LNS.
6. The encapsulated packets are sent to the peer LNS through the packet data network where they will be un-encapsulated.

## Configuring Attribute-based L2TP Support for HA Mobile IP

This section provides a list of the steps required to configure attribute-based L2TP support for use with HA Mobile IP applications. Each step listed refers to a different section containing the specific instructions for completing the required procedure.



**Important:** These instructions assume that the system was previously configured to support subscriber data sessions as an HA.

- Step 1** Configure the subscriber profiles according to the information and instructions located in the *Configuring Subscriber Profiles for L2TP Support* section of this chapter.
- Step 2** Configure one or more LAC services according to the information and instructions located in the *Configuring LAC Services* section of this chapter.

- Step 3** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

## Configuring Subscriber Profiles for L2TP Support

This section provides information and instructions on the following procedures:

- [RADIUS and Subscriber Profile Attributes Used](#)
- [Configuring Local Subscriber Profiles for L2TP Support](#)
- [Configuring Local Subscriber](#)
- [Verifying the L2TP Configuration](#)



**Important:** Since the instructions for configuring subscribers differ between RADIUS server applications, this section only provides the individual attributes that can be added to the subscriber profile. Refer to the documentation that shipped with your RADIUS server for instructions on configuring subscribers.


### RADIUS and Subscriber Profile Attributes Used

Attribute-based L2TP tunneling is supported through the use of attributes configured in subscriber profiles stored either locally on the system or remotely on a RADIUS server. The following table describes the attributes used in support of LAC services. These attributes are contained in the standard and VSA dictionaries.

Table 32. Subscriber Attributes for L2TP Support

RADIUS Attribute	Local Subscriber Attribute	Description	Variable
Tunnel-Type	tunnel l2tp	Specifies the type of tunnel to be used for the subscriber session	L2TP
Tunnel-Server-Endpoint	tunnel l2tp peer-address	Specifies the IP address of the peer LNS to connect tunnel to.	IPv4 address in dotted-decimal format, enclosed in quotation marks
Tunnel-Password	tunnel l2tp secret	Specifies the shared secret between the LAC and LNS.	Alpha and or numeric string from 1 to 63 characters, enclosed in quotation marks
Tunnel-Private-Group-ID	tunnel l2tp tunnel-context	Specifies the name of the destination context configured on the system in which the LAC service(s) to be used are located.  <div data-bbox="552 1602 609 1667" data-label="Image"> </div> <b>Important:</b> If the LAC service and egress interface are configured in the same context as the core service or HA service, this attribute is not needed.	Alpha and or numeric string from 1 to 63 characters, enclosed in quotation marks



RADIUS Attribute	Local Subscriber Attribute	Description	Variable
Tunnel-Preference	tunnel l2tp preference	Configures the priority of each peer LNS when multiple LNS nodes are configured.   <b>Important:</b> This attribute is only used when the <b>loadbalance-tunnel-peers</b> parameter or <b>SN-Tunnel-Load-Balancing</b> attribute configured to prioritized.	Integer from 1 to 65535
SN-Tunnel-Load-Balancing	loadbalance-tunnel- peer	A vendor-specific attribute (VSA) used to provides a selection algorithm defining how an LNS node is selected by the RADIUS server when multiple LNS peers are configured within the subscriber profile.	<ul style="list-style-type: none"> <li>• <b>Random</b> - Random LNS selection order, the <b>Tunnel-Preference</b> attribute is not used in determining which LNS to select.</li> <li>• <b>Balanced</b> - LNS selection is sequential balancing the load across all configured LNS nodes, the <b>Tunnel-Preference</b> attribute is not used in determining which LNS to select.</li> <li>• <b>Prioritized</b> - LNS selection is made based on the priority assigned in the <b>Tunnel-Preference</b> attribute.</li> </ul>
Client-Endpoint	local-address	Specifies the IP address of a specific LAC service configured on the system that to use to facilitate the subscriber's L2TP session. This attribute is used when multiple LAC services are configured.	IPv4 address in dotted decimal notation. (xxx.xxx.xxx.xxx)

## RADIUS Tagging Support

The system supports RADIUS attribute tagging for tunnel attributes. These “tags” organize together multiple attributes into different groups when multiple LNS nodes are defined in the user profile. Tagging is useful to ensure that the system groups all the attributes used for a specific server. If attribute tagging is not supported by your specific RADIUS server, the system implicitly organizes the attributes in the order that they are listed in the access accept packet.

## Configuring Local Subscriber Profiles for L2TP Support

This section provides information and instructions for configuring local subscriber profiles on the system to support L2TP.



**Important:** The configuration of RADIUS-based subscriber profiles is not discussed in this document. Please refer to the documentation supplied with your RADIUS server for further information.



**Important:** This section provides the minimum instruction set for configuring local subscriber profile for L2TP support on the system. For more information on commands that configure additional parameters and options, refer to the *LAC Service Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

To configure the system to provide L2TP support to subscribers:

- Step 1** Configure the “Local” subscriber with L2TP tunnel parameters and the load balancing parameters with action by applying the example configuration in the *Configuring Local Subscriber* section.
- Step 2** Verify your L2TP configuration by following the steps in the *Verifying the L2TP Configuration* section.
- Step 3** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

## Configuring Local Subscriber

Use the following example to configure the Local subscriber with L2TP tunnel parameters. Optionally you can configure load balancing between multiple LNS servers:

```
configure

context <ctxt_name> [-noconfirm]

    subscriber name <subs_name>

        tunnel l2tp peer-address <lns_ip_address> [ preference <integer> | [ encrypted ]
secret <secret_string> | tunnel-context <context_name> | local-address <local_ip_address>
    }

    load-balancing { random | balanced | prioritized }

end
```

Notes:

- <ctxt\_name> is the system context in which you wish to configure the subscriber profile.
- <lns\_ip\_address> is the IP address of LNS server node and <local\_ip\_address> is the IP address of system which is bound to LAC service.

## Verifying the L2TP Configuration

These instructions are used to verify the L2TP configuration.

- Step 1** Verify that your L2TP configurations were configured properly by entering the following command in Exec Mode in specific context:

```
show subscriber configuration username user_name
```

The output of this command is a concise listing of subscriber parameter settings as configured.

## Tunneling All Subscribers in a Specific Context Without Using RADIUS Attributes

As with other services supported by the system, values for subscriber profile attributes not returned as part of a RADIUS Access-Accept message can be obtained using the locally configured profile for the subscriber named default. The subscriber profile for default must be configured in the AAA context (i.e. the context in which AAA functionality is configured).

As a time saving feature, L2TP support can be configured for the subscriber named default with no additional configuration for RADIUS-based subscribers. This is especially useful when you have separate source/AAA contexts for specific subscribers.

To configure the profile for the subscriber named default, follow the instructions above for configuring a local subscriber and enter the name default.

## Configuring LAC Services



**Important:** Not all commands, keywords and functions may be available. Functionality is dependent on platform and license(s).

This section provides information and instructions for configuring LAC services on the system allowing it to communicate with peer LNS nodes.



**Important:** This section provides the minimum instruction set for configuring LAC service support on the system. For more information on commands that configure additional parameters and options, refer to the *LAC Service Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

To configure the LAC services on system:

- Step 1** Configure the LAC service on system and bind it to an IP address by applying the example configuration in the *Configuring LAC Service* section.
- Step 2** *Optional.* Configure LNS peer information if the Tunnel-Service-Endpoint attribute is not configured in the subscriber profile or PDSN compulsory tunneling is supported by applying the example configuration in the *Configuring LNS Peer* section.
- Step 3** Verify your LAC configuration by following the steps in the *Verifying the LAC Service Configuration* section.
- Step 4** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

## Configuring LAC Service

Use the following example to create the LAC service and bind the service to an IP address:

```
configure
  context <dst_ctxt_name> [-noconfirm]
    lac-service <service_name>
      bind address <ip_address>
    end
```

Notes:

- <dst\_ctxt\_name> is the destination context where you want to configure the LAC service.

## Configuring LNS Peer

Use the following example to configure the LNS peers and load balancing between multiple LNS peers:

```
configure

context <dst_ctxt_name> [ -noconfirm ]

lac-service <service_name>

    tunnel selection-key tunnel-server-auth-id

    peer-lns <ip_address> [encrypted] secret <secret> [crypto-map <map_name>
{[encrypted] isakmp-secret <secret> }] [description <text>] [ preference <integer>]

    load-balancing { random | balanced | prioritized }

end
```

Notes:

- <dst\_ctxt\_name> is the destination context where the LAC service is configured.

## Verifying the LAC Service Configuration

These instructions are used to verify the LAC service configuration.

- Step 1** Verify that your LAC service configurations were configured properly by entering the following command in Exec Mode in specific context:

```
show lac-service name service_name
```

The output given below is a concise listing of LAC service parameter settings as configured.

```
Service name: vpn1

Context:                               isp1

Bind:                                  Done

Local IP Address:                      192.168.2.1

First Retransmission Timeout: 1 (secs)

Max Retransmission Timeout: 8 (secs)

Max Retransmissions: 5

Max Sessions: 500000                   Max Tunnels: 32000

Max Sessions Per Tunnel: 512

Data Sequence Numbers: Enabled        Tunnel Authentication: Enabled
```

## ■ Configuring LAC Services

Keep-alive interval:	60	Control receive window:	16
Max Tunnel Challenge Length:	16		
Proxy LCP Authentication:	Enabled		
Load Balancing:	Random		
Service Status:	Started		
Newcall Policy:	None		

## Modifying PDSN Services for L2TP Support

PDSN service modification is required for compulsory tunneling and optional for attribute-based tunneling.

For attribute-based tunneling, a configuration error could occur such that upon successful authentication, the system determines that the subscriber session requires L2TP but can not determine the name of the context in which the appropriate LAC service is configured from the attributes supplied. As a precautionary, a parameter has been added to the PDSN service configuration options that will dictate the name of the context to use. It is strongly recommended that this parameter be configured.

This section contains instructions for modifying the PDSN service configuration for either compulsory or attribute-based tunneling.



**Important:** This section provides the minimum instruction set for modifying PDSN service for L2TP support on the system. For more information on commands that configure additional parameters and options, refer to the *LAC Service Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

To configure the LAC services on system:

- Step 1** Modify the PDSN service to support L2TP by associating LAC context and defining tunnel type by applying the example configuration in the *Modifying PDSN Service* section.
- Step 2** Verify your configuration to modify PDSN service by following the steps in the *Verifying the PDSN Service for L2TP Support* section.
- Step 3** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

### Modifying PDSN Service

Use the following example to modify the PDSN service to support L2TP by associating LAC context and defining tunnel type:

```
configure

context <source_ctxt_name> [ -noconfirm ]

pdsn-service <pdsn_service_name>

ppp tunnel-context <lac_context_name>

ppp tunnel-type { l2tp | none }

end
```

Notes:

- *<source\_ctxt\_name>* is the name of the source context containing the PDSN service, which you want to modify for L2TP support.

- *<pdsn\_service\_name>* is the name of the pre-configured PDSN service, which you want to modify for L2TP support.
- *<lac\_context\_name>* is typically the destination context where the LAC service is configured.

## Verifying the PDSN Service for L2TP Support

These instructions are used to verify the PDSN service configuration.

**Step 1** Verify that your PDSN is configured properly by entering the following command in Exec Mode in specific context:

```
show pdsn-service name pdsn_service_name
```

The output of this command is a concise listing of PDSN service parameter settings as configured.



## Modifying APN Templates to Support L2TP

This section provides instructions for adding L2TP support for APN templates configured on the system.



**Important:** This section provides the minimum instruction set for configuring LAC service support on the system. For more information on commands that configure additional parameters and options, refer to the *LAC Service Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

To configure the LAC services on system:

- Step 1** Modify the APN template to support L2TP with LNS server address and other parameters by applying the example configuration in the *Assigning LNS Peer Address in APN Template* section.
- Step 2** Optional. If L2TP will be used to tunnel transparent IP PDP contexts, configure the APN's outbound username and password by applying the example configuration in the *Configuring Outbound Authentication* section.
- Step 3** Verify your APN configuration by following the steps in the *Verifying the APN Configuration* section.
- Step 4** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

### Assigning LNS Peer Address in APN Template

Use following example to assign LNS server address with APN template:

```
configure

context <dst_ctxt_name> [-noconfirm]

    apn <apn_name>

        tunnel l2tp [ peer-address <lns_address> [ [ encrypted ] secret <l2tp_secret> ]
[ preference <integer> ] [ tunnel-context <l2tp_context_name> ] [ local-address
<local_ip_address> ] [ crypto-map <map_name> { [ encrypted ] isakmp-secret
<crypto_secret> } ]

    end
```

Notes:

- <dst\_ctxt\_name> is the name of system destination context in which the APN is configured.
- <apn\_name> is the name of the pre-configured APN template which you want to modify for the L2TP support.
- <lns\_address> is the IP address of LNS server node and <local\_ip\_address> is the IP address of system which is bound to LAC service.

## Configuring Outbound Authentication

Use the following example to configure the LNS peers and load balancing between multiple LNS peers:

```
configure
  context <dst_ctxt_name> [ -noconfirm ]
    apn <apn_name>
      outbound { [ encrypted ] password <pwd> | username <name> }
    end
```

Notes:

- <dst\_ctxt\_name> is the destination context where APN template is configured.
- <apn\_name> is the name of the pre-configured APN template which you want to modify for the L2TP support.

## Verifying the APN Configuration

These instructions are used to verify the APN configuration.

**Step 1** Verify that your APN configurations were configured properly by entering the following command in Exec Mode in specific context:

```
show apn name apn_name
```

The output is a concise listing of APN parameter settings as configured.


# Appendix J

## L2TP Network Server

---

This chapter describes the support for Layer 2 Tunneling Protocol (L2TP) Network Server (LNS) functionality on Cisco® ASR 5x00 chassis and explains how it is configured. The product Administration Guides provide examples and procedures for configuration of basic services on the system. It is recommended that you select the configuration example that best meets your service model, and configure the required elements for that model, as described in the respective product Administration Guide, before using the procedures in this chapter.


---

 **Important:** The Layer 2 Tunneling Protocol (L2TP) Network Server (LNS) is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

---

When enabled through the session license and feature use key, LNS functionality is configured as context-level services on the system. LNS services support the termination of L2TP encapsulated tunnels from L2TP Access Concentrators (LACs) in accordance with RFC 2661.

---

 **Important:** The LNS service uses UDP ports 13660 through 13668 as the source port for receiving packets from the LAC. You can force the LNS to only use the standard L2TP port (UDP Port 1701) with the **single-port-mode** LNS service configuration mode command. Refer to the Command Line Interface Reference for more information on this command.

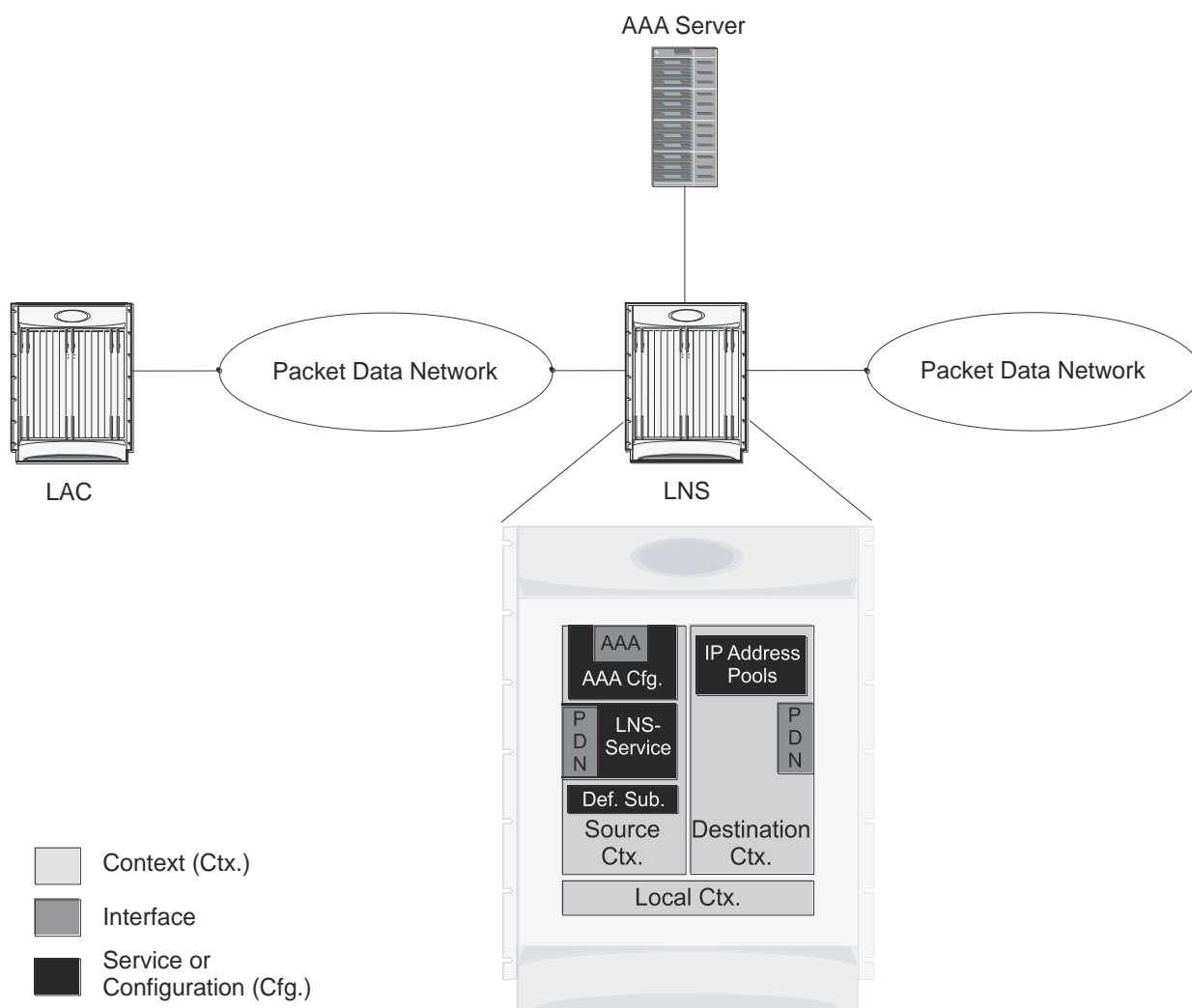
---

## LNS Service Operation

As mentioned previously, LNS functionality on the system is configured via context-level services. LNS services can be configured in the same context as other services supported on the system or in its own context. Each context can support multiple LNS services.

One of the most simple configuration that can be implemented on the system to support Simple IP data applications requires that two contexts (one source and one destination) be configured on the system as shown in the following figure.

Figure 69. LNS Configuration Example



The source context facilitates the LNS service(s) and the PDN and AAA interfaces. The PDN interface is bound to the LNS service and connects L2TP tunnels and sessions from one or more peer LACs. The source context is also be configured to provide AAA functionality for subscriber sessions. The destination context facilitates the packet data network interface(s) and can optionally be configured with pools of IP addresses for assignment to subscriber sessions.

In this configuration, the LNS service in the source context terminates L2TP tunnels from peer LACs and routes the subscriber session data through the destination context to and from a packet data network such as the Internet or a home network.

## Information Required

Prior to configuring the system as shown in figure above, a minimum amount of information is required. The following sections describe the information required to configure the source and destination contexts.

### Source Context Configuration

The following table lists the information that is required to configure the source context.

**Table 33. Required Information for Source Context Configuration**

Required Information	Description
Source context name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the source context will be recognized by the system.
PDN Interface Configuration	
PDN interface name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. These PDN interfaces facilitates the L2TP tunnels/sessions from the LAC and are configured in the source context.
IP address and subnet	These will be assigned to the PDN interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the source context and are used to bind logical PDN interfaces.
Gateway IP address	Used when configuring static routes from the PDN interface(s) to a specific network.
LNS service Configuration	
LNS service name	This is an identification string between 1 and 63 characters (alpha and/or numeric) by which the LNS service will be recognized by the system. Multiple names are needed if multiple LNS services will be used. LNS services are configured in the source context.
Authentication protocols used	Specifies how the system handles authentication: using a protocol (such as CHAP, PAP, or MSCHAP), or not requiring any authentication.
Domain alias for NAI-construction	Specifies a context name for the system to use to provide accounting functionality for a subscriber session. This parameter is needed only if the system is configured to support no authentication.

Required Information	Description
Maximum number of sessions per tunnel	This defines the maximum number of sessions supported by each tunnel facilitated by the LNS service. The number can be configured to any integer value from 1 to 65535. The default is 65535.
Maximum number of tunnels	This defines the maximum number of tunnels supported by the LNS service. The number can be configured to any integer value from 1 to 32000. The default is 32000.
Peer LAC	IP address or network prefix and mask: The IP address of a specific peer LAC for which the LNS service terminates L2TP tunnels. The IP address must be expressed in dotted decimal notation. Multiple peer LACs can be configured. Alternately, to simplify configuration, a group of peer LACs can be specified by entering a network prefix and a mask.
	Secret: The shared secret used by the LNS to authenticate the peer LAC. The secret can be from 1 to 256 alpha and/or numeric characters and is case sensitive.
AAA Interface Configuration	
AAA interface name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. AAA interfaces will be configured in the source context.
IP address and subnet	These will be assigned to the AAA interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	A single physical port can facilitate multiple interfaces.
Physical port description	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the source context and are used to bind logical AAA interfaces.
Gateway IP address	Used when configuring static routes from the AAA interface(s) to a specific network.
RADIUS Server Configuration	
RADIUS Authentication server	IP Address: Specifies the IP address of the RADIUS authentication server the source context will communicate with to provide subscriber authentication functions. Multiple addresses are needed if multiple RADIUS servers will be configured. RADIUS authentication servers are configured within the source context. Multiple servers can be configured and each assigned a priority.
	Shared Secret: The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the RADIUS authentication server and the source context. A shared secret is needed for each configured RADIUS server.
	UDP Port Number: Specifies the port used by the source context and the RADIUS authentication server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1812.

Required Information	Description
RADIUS Accounting server	<b>IP Address:</b> Specifies the IP address of the RADIUS accounting server that the source context will communicate with to provide subscriber accounting functions. Multiple addresses are needed if multiple RADIUS servers will be configured. RADIUS accounting servers are configured within the source context. Multiple servers can be configured and each assigned a priority.
	<b>Shared Secret:</b> The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the RADIUS accounting server and the source context. A shared secret is needed for each configured RADIUS server.
	<b>UDP Port Number:</b> Specifies the port used by the source context and the RADIUS Accounting server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1813.
RADIUS attribute NAS Identifier	Specifies the name by which the source context will be identified in the Access-Request message(s) it sends to the RADIUS server. The name must be between 1 and 32 alpha and/or numeric characters and is case sensitive.
RADIUS NAS IP address	Specifies the IP address of the source context's AAA interface. A secondary IP address interface can optionally be configured.
Default Subscriber Configuration	
"Default" subscriber's IP context name	Specifies the name of the egress context on the system that facilitates the PDN ports. <b>NOTE:</b> For this configuration, the IP context name should be identical to the name of the destination context.

## Destination Context Configuration

The following table lists the information that is required to configure the destination context.

**Table 34. Required Information for Destination Context Configuration**

Required Information	Description
Destination context name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the destination context will be recognized by the system. <b>NOTE:</b> For this configuration, the destination context name should <b>not</b> match the domain name of a specific domain.
PDN Interface Configuration	
PDN interface name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. PDN interfaces are used to connect to a packet network and are configured in the destination context.
IP address and subnet	These will be assigned to the PDN interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.

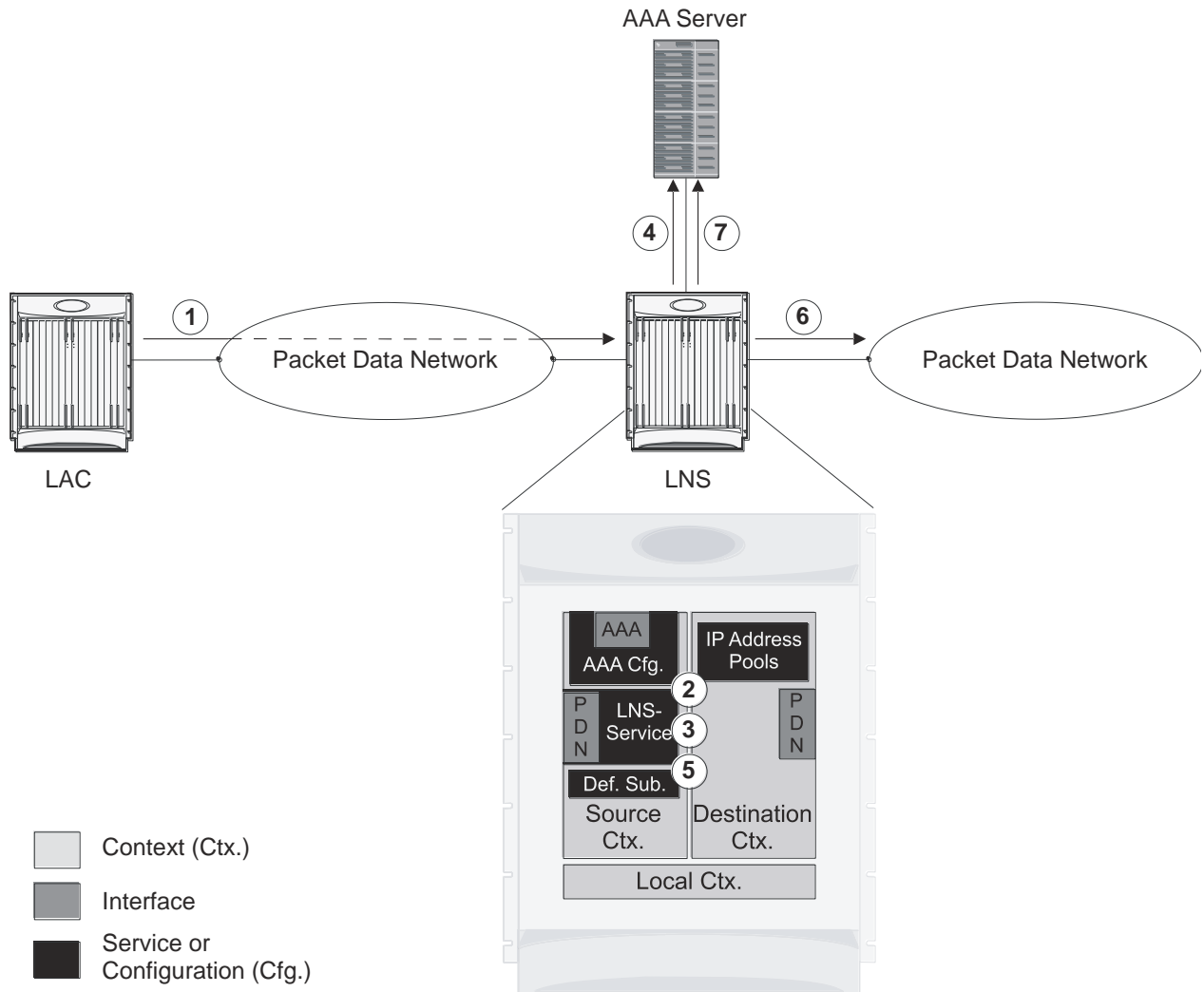
Required Information	Description
Physical port number	A single physical port can facilitate multiple interfaces.
Physical port description(s)	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions will be needed if multiple ports will be used. Physical ports are configured within the destination context and are used to bind logical PDN interfaces.
Gateway IP address(es)	Used when configuring static routes from the PDN interface(s) to a specific network.
IP Address Pool Configuration (optional)	
IP address pool name(s)	If IP address pools will be configured in the destination context(s), names or identifiers will be needed for them. The pool name can be between 1 and 31 alpha and/or numeric characters and is case sensitive.
IP pool addresses	An initial address and a subnet, or a starting address and an ending address, are required for each configured pool. The pool will then consist of every possible address within the subnet, or all addresses from the starting address to the ending address. The pool can be configured as public, private, or static.

## How This Configuration Works

The following figure and the text that follows describe how this LNS service configuration with a single source and destination context would be used by the system to terminate an L2TP tunnel.



Figure 70. Call Processing Using a Single Source and Destination Context



1. An L2TP tunnel request from a peer LAC is received by the LNS service. The tunnel is to facilitate a subscriber session.
2. The LAC and LNS establish the L2TP tunnel according to the procedures defined in RFC 2661. Once the L2TP tunnel is established, subscriber L2TP sessions can be established.
3. The LNS service determines which context to use in providing AAA functionality for the subscriber session if authentication is enabled for the LNS service. For more information on this process, refer *How the System Selects Contexts in System Administration Guide*. For this example, the result of this process is that LNS service determined that AAA functionality should be provided by the Source context.
4. The system communicates with the AAA server specified in the Source context's AAA configuration to authenticate the subscriber.
5. Upon successful authentication, the LNS service terminates the subscriber's PPP datagrams from the L2TP session and the system determines which egress context to use for the subscriber session. For more information on egress context selection process, refer *How the System Selects Contexts in System Administration Guide*.

The system determines that the egress context is the destination context based on the configuration of either the Default subscriber's ip-context name or from the SN-VPN-NAME or SN1-VPN-NAME attributes that is configured in the subscriber's RADIUS profile.

6. Data traffic for the subscriber session is routed through the PDN interface in the Destination context.
7. Accounting information for the session is sent to the AAA server over the AAA interface.

## Configuring the System to Support LNS Functionality

Many of the procedures required to configure the system to support LNS functionality are provided in the System Administration Guide. The System Administration Guide provides information and procedures for configuring contexts, interfaces and ports, AAA functionality, and IP address pools on the system.

This section provides information and instructions for configuring LNS services on the system allowing it to communicate with peer LAC nodes.



**Important:** This section provides the minimum instruction set for configuring an LNS service allowing the system to terminate L2TP tunnels and process data sessions. For more information on commands that configure additional LNS service properties, refer LNS Configuration Mode Commands chapter in Command Line Interface Reference.

To configure the system to provide access control list facility to subscribers:

- Step 1** Create the LNS service and bind it to an interface IP address by applying the example configuration in the *Creating and Binding LNS Service* section.
- Step 2** Specify the authentication parameters for LNS service by applying the example configuration in the *Configuring Authentication Parameters for LNS Service* section.
- Step 3** Configure the maximum number of tunnels supported by the LNS service and maximum number of sessions supported per tunnel by applying the example configuration in the *Configuring Tunnel and Session Parameters for LNS Service* section.
- Step 4** Configure peer LACs for the LNS service by applying the example configuration in the *Configuring Tunnel and Session Parameters for LNS Service* section.
- Step 5** *Optional.* Specify the domain alias designated for the context which the LNS service uses for AAA functionality by applying the example configuration in the *Configuring Domain Alias for AAA Subscribers* section.
- Step 6** Verify your LNS service configuration by following the steps in the *Verifying the LNS Service Configuration* section.
- Step 7** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

## Creating and Binding LNS Service

Use the following example to create the LNS service and bind the IP address to it:

```
configure

context <dest_ctxt_name> -noconfirm

    lns-service <lns_svc_name> -noconfirm

        bind address <ip_address> [ max-subscribers <max_subscriber> ]
```

```
end
```

Notes:

- LNS service has to be configured in destination context.
- Bind address is the interface address that is to serve as an L2TP PDN interface.
- Multiple addresses on the same IP interface can be bound to different LNS services. However, each address can be bound to only one LNS service. In addition, the LNS service can not be bound to the same interface as other services such as a LAC service.

## Configuring Authentication Parameters for LNS Service

Use the following example to authentication parameters for LNS service:

```
configure
  context <dest_ctxt_name>
    lns-service <lns_svc_name>
      authentication { { [ allow-noauth | chap <pref> | mschap <pref> | | pap <pref> ]
} | msid-auth }
    end
```

Note:

- For more information on authentication procedure and priorities, refer **authentication** command section in LNS Configuration Mode Commands chapter of Command Line Interface Reference.

## Configuring Tunnel and Session Parameters for LNS Service

Use the following example to configure the tunnel and session parameters for LNS service:

```
configure
  context <dest_ctxt_name>
    lns-service <lns_svc_name>
      max-tunnel <max_tunnels>
      max-session-per-tunnel <max_sessions>
    end
```

Note:

- For more information on tunnel and session related parameters, refer LNS Configuration Mode Commands chapter of Command Line Interface Reference.

## Configuring Peer LAC servers for LNS Service

Use the following example to configure the peer LAC servers for LNS service:

```
configure

context <dest_ctxt_name>

    lns-service <lns_svc_name>

        peer-lac { <lac_ip_address> | <ip_address>/<mask> } [ encrypted ] secret
        <secret_string> [ description <desc_text> ]

    end
```

Note:

- Multiple LACs can be configured with this command. For more information, refer LNS Configuration Mode Commands chapter of Command Line Interface Reference.

## Configuring Domain Alias for AAA Subscribers

Use the following example to create the LNS service and bind the IP address to it:

```
configure

context <dest_ctxt_name> -noconfirm

    lns-service <lns_svc_name> -noconfirm

        nai-construct domain <domain_alias>

    end
```

Note:

- If this command is enabled, an NAI is constructed for the subscriber in the event that their mobile node does not negotiate CHAP, PAP, or MSCHAP.
- If this option is selected, no further attempts are made to authenticate the user. Instead, the constructed NAI is used for accounting purposes.



**Important:** This command should only be used if the LNS service is configured to allow “no authentication” using the **authentication allow-noauth** command.

## Verifying the LNS Service Configuration

These instructions are used to verify the LNS service configuration.

**Step 1** Verify that your LNS service configuration by entering the following command in Exec Mode:

```
show lns-service name service_name
```

The output of this command displays the configuration of the LNS service and should appear similar to that shown below.

```

Service name: testlns

Context:                test

Bind:                   Not Done

Local IP Address:       0.0.0.0

First Retransmission Timeout: 1 (secs)

Max Retransmission Timeout: 8 (secs)

Max Retransmissions:    5

Setup Timeout:          60 (secs)

Max Sessions:           500000      Max
Tunnels:                 32000

Max Sessions Per Tunnel: 65535

Keep-alive Interval:    60          Control Receive Window: 16

Data Sequence Numbers:  Enabled

Tunnel Authentication:  Enabled

Tunnel Switching:      Enabled

Max Tunnel Challenge Length: 16

PPP Authentication:     CHAP 1 PAP 2

Allow Noauthentication:  Disabled    MSID
Authentication:         Disabled

No NAI Construct Domain defined

No Default Subscriber defined

IP Src Violation Reneg Limit: 5

IP Src Violation Drop Limit: 10

IP Src Violation Period: 120 (secs)

Service Status:         Not started

Newcall Policy:         None

```

# Appendix K

## Mobile IP Registration Revocation

---

This chapter describes Registration Revocation for Mobile-IP and Proxy Mobile-IP and explains how it is configured. The product administration guides provide examples and procedures for configuration of basic services on the system. It is recommended that you select the configuration example that best meets your service model and configure the required elements for that model, as described in this administration guide before using the procedures in this chapter.



**Important:** This license is enabled by default; however, not all features are supported on all platforms and other licenses may be required for full functionality as described in this chapter.

---

## Overview


Registration Revocation is a general mechanism whereby either the HA or the FA providing Mobile IP functionality to the same mobile node can notify the other mobility agent of the termination of a binding. This functionality provides the following benefits:

- Timely release of Mobile IP resources at the FA and/or HA
- Accurate accounting
- Timely notification to mobile node of change in service

Mobile IP Registration Revocation can be triggered at the FA by any of the following:

- Session terminated with mobile node for whatever reason
- Session renegotiation
- Administrative clearing of calls
- Session Manager software task outage resulting in the loss of FA sessions (sessions that could not be recovered)

---

 **Important:** Registration Revocation functionality is also supported for Proxy Mobile IP. However, only the HA can initiate the revocation for Proxy-MIP calls.

---


Mobile IP Registration Revocation can be triggered at the HA by any of the following:

- Administrative clearing of calls
- Inter-Access Gateway handoff. This releases the binding at the previous access gateway/FA
- Session Manager software task outage resulting in the loss of FA sessions (for sessions that could not be recovered)
- Session Idle timer expiry (when configured to send Revocation)
- Any other condition under which a binding is terminated due to local policy (duplicate IMSI detected, duplicate home address requested, etc.)

The FA and the HA negotiate Registration Revocation support when establishing a Mobile IP call. Revocation support is indicated to the Mobile Node (MN) from the FA by setting the 'X' bit in the Agent Advertisement to MN. However the MN is not involved in negotiating the Revocation for a call or in the Revocation process. It only gets notified about it. The X bit in the Agent Advertisements is just a hint to the MN that revocation is supported at the FA but is not a guarantee that it can be negotiated with the HA

At the FA, if revocation is enabled and a FA-HA SPI is configured, the Revocation Support extension is appended to the RRQ received from the MN and protected by the FA-HA Authentication Extension. At the HA, if the RRQ is accepted, and the HA supports revocation, the HA responds with an RRP that includes the Revocation Support extension. Revocation support is considered to be negotiated for a binding when both sides have included a Revocation Support Extension during a successful registration exchange.

---

 **Important:** The Revocation Support Extension in the RRQ or RRP must be protected by the FA-HA Authentication Extension. Therefore, an FA-HA SPI must be configured at the FA and the HA for this to succeed.

---

If revocation is enabled at the FA, but an FA-HA SPI is not configured at the FA for a certain HA, then FA does not send Revocation Support Extension for a call to that HA. Therefore, the call may come up without Revocation support negotiated.



If the HA receives an RRQ with Revocation Support Extension, but not protected by FA-HA Auth Extension, it will be rejected with “FA Failed Authentication” error.

If the FA receives a RRP with Revocation Support Extension, but not protected by FA-HA Auth Extension, it will be rejected with “HA Failed Authentication” error.


Also note that Revocation support extension is included in the initial, renewal or handoff RRQ/RRP messages. The Revocation extension is not included in a Deregistration RRQ from the FA and the HA will ignore them in any Deregistration RRQs received.


## Configuring Registration Revocation

Support for MIP Registration Revocation requires the following configurations:

- **FA service(s):** Registration Revocation must be enabled and operational parameters optionally configured.
- **HA service(s):** Registration Revocation must be enabled and operational parameters optionally configured.

---

 **Important:** These instructions assume that the system was previously configured to support subscriber data sessions for a core network service with FA and/or an HA according to the instructions described in the respective product Administration Guide.

 **Important:** Commands used in the configuration samples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the *Command Line Interface Reference* for complete information regarding all commands.

---

## Configuring FA Services

Configure FA services to support MIP Registration Revocation by applying the following example configuration:

```
configure

context <context_name>

    fa-service <fa_service_name>

        revocation enable

        revocation max-retransmission <number>

        revocation retransmission-timeout <time>

    end
```

Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

## Configuring HA Services

Configure HA services to support MIP Registration Revocation by applying the following example configuration:

```
configure

context <context_name>

    ha-service <ha_service_name>
```

```
revocation enable

revocation max-retransmission <number>

revocation retransmission-timeout <time>

end
```

Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.



# Appendix L

## Multimedia Broadcast and Multicast Service

---

This chapter provides information on Multimedia Broadcast and Multicast Service (MBMS) functionality on GGSN. The product Administration Guides provide examples and procedures for configuration of basic services on the system. It is recommended that you select the configuration example that best meets your service model, and configure the required elements for that model, as described in the respective product Administration Guide, before using the procedures in this chapter.



**Important:** The features described in this chapter are only available if you have purchased and installed MBMS feature support license on your chassis.

---

This chapter discusses following topics for MBMS support:

- [Introduction](#)
- [Supported Standards](#)
- [Supported Networks and Platforms](#)
- [Services and Application in MBMS](#)
- [How MBMS Works](#)
- [MBMS Configuration](#)
- [Save the Configuration](#)
- [Managing Your Configuration](#)
- [Gathering MBMS Statistics](#)

# Introduction

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 with a suitable method for mass communications.

MBMS functionality on the system is provided by an existing GGSN service and is enabled by a valid services license.

The main features supported by the Multimedia Broadcast & Multicast Services are:

- Individual user network control functions and provide forward MBMS user data to SGSN



**Important:** The Cisco chassis supports 225 downlink SGSNs per MBMS Bearer Service through NPU assisted data flow processing. NPU assisted data processing is available on the systems with release 8.1 or later only.

- Support for intra-GGSN and inter-GGSN mobility procedures
- Generate charging data per multicast service for each user for both prepaid and post paid subscribers.
- Multicast proxy-host functionality
- Support for MBMS-specific Gmb messages
- Authentication of MBMS flow-ids using a MBMS controller
- Establishment and tear-down of MBMS bearer paths using the multicast framework
- Support for framing HDLC-like and segment based framing
- Accounting for the MBMS flows to charge the originator of the content

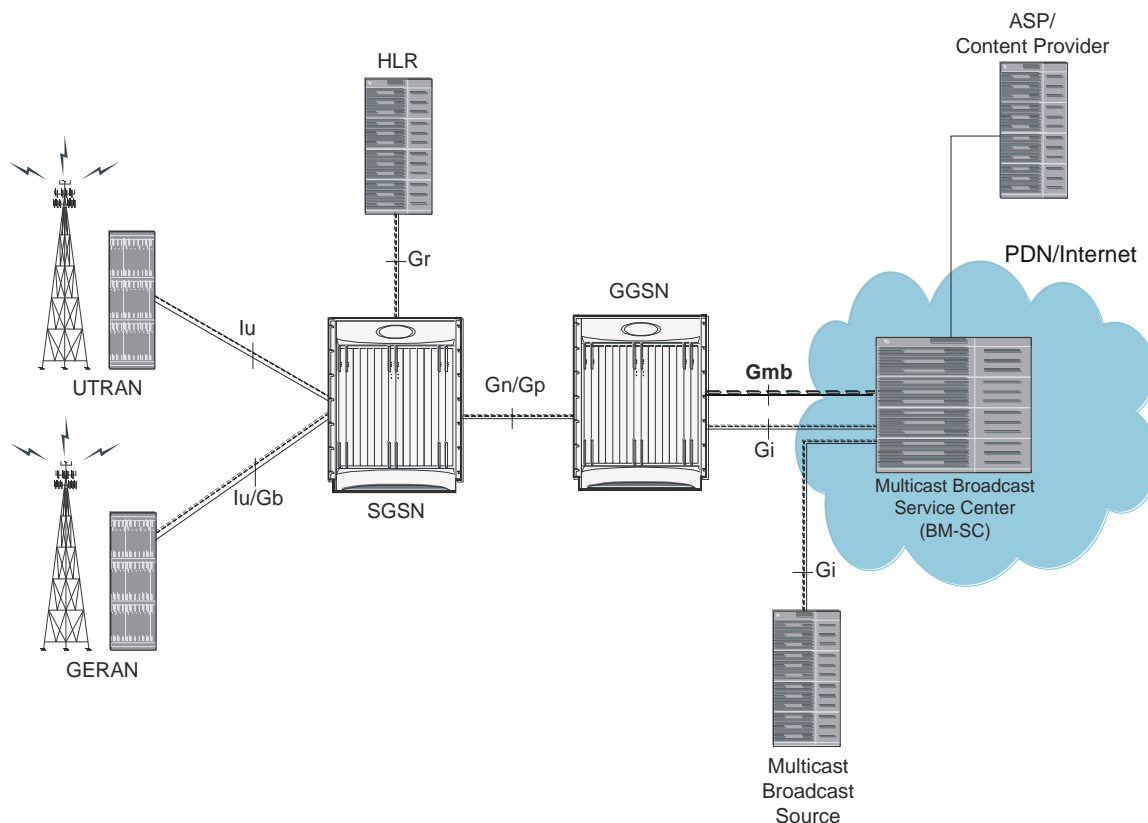
This service provides two mode of operations:

- MBMS Broadcast Mode
- MBMS Multicast Mode

A broadcast mode is a unidirectional point-to-multipoint service in which data is transmitted from a single source to multiple terminals (UE/MS) in the associated broadcast service area/cell area. The transmitted data can be text to light multimedia services (Audio, Video etc). On the other hand multicast mode is a unidirectional point-to-multipoint service in which data is transmitted from a single source to a pre-defined multicast group of users that are subscribed to the specific multicast service and have joined the multicast group in the associated multicast service area.

The following figure shows the reference architecture of MBMS service in UMTS network.

Figure 71. MBMS Reference Architecture in UMTS network



The GGSN provides the following functionality to perform MBMS services:

- serves as an entry point for IP multicast traffic as MBMS data. It provides establishment of bearer plan and tear-down of the established bearer plan upon notification from the BM-SC.
- provides functionality to receive MBMS specific IP multicast traffic and to route this data to the proper GTP tunnels set-up as part of the MBMS bearer service.
- provides features, that are not exclusive to MBMS, for the MBMS bearer service, like charging data collection, flow-based charging, optional message screening etc.

MBMS is able to use NPU assisted MBMS data flow processing on chassis so that system can relieve the Session Manager to provide better performance and processing. Currently with NPU assisted data processing, the Cisco chassis can support 225 SGSNs per MBMS Bearer Service for downlink of MBMS data.

## Supported Standards

Support for the following standards and requests for comments (Rafts) have been added with the MBMS functionality:

- 3GPP TS 22.146: Multimedia Broadcast/Multicast Service; Stage 1 (Release 6)
- 3GPP TS 22.246: MBMS user services; Stage 1 (Release 6)
- 3GPP TS 23.246: MBMS; Architecture and functional description (Release 6)
- 3GPP TS 26.346: MBMS; Protocols and codecs (Release 6)
- 3GPP TS 33.246: Security of Multimedia Broadcast/Multicast Service
- 3GPP TS 32.251: Telecommunication management; Charging management; Packet Switched (PS) domain charging
- 3GPP TS 32.273: Telecommunication management; Charging management; Multimedia Broadcast and Multicast Service (MBMS) charging
- RFC 3588, Diameter Base Protocol



# Supported Networks and Platforms

This feature supports all Cisco chassis running StarOS Release 8.0 or later with GGSN service for the core network services.

## License Information

## Services and Application in MBMS

MBMS service can be used as an enabler for various data streaming services. Compared to traditional broadcast services like cell broadcast, MBMS provides multimedia capabilities with relatively high data rates and considerably greater multimedia capabilities.

Some of the applications for MBMS are:

- News clips
- Audio streams
- Combined audio and picture/video clips
- Video distribution services, either via streaming, carousel, or download methods
- Localized services like tourist information, weather alerts etc.
- Content distribution
- Game delivery

The charging of the MBMS bearer service can be done based on events, content, or flows.

MBMS provides the authentication, key distribution, and data protection for the multicast service users.

## MBMS References and Entities

Following are the major components and entities required for MBMS service.

### Gmb Reference

The Gmb reference point handles the broadcast multicast service center (BM-SC) related signaling, which includes the user specific and bearer service messages.

MBMS bearer service specific Gmb signaling includes:

- MBMS bearer context establishment by GGSN and registering of GGSN at BM-SC.
- Release of MBMS bearer context at GGSN and de-registration of GGSN from the BM-SC.
- Session start/stop indication from BM-SC to GGSN including session attributes like QoS or MBMS service area.

User specific Gmb signaling includes:

- BM-SC authorization of user specific MBMS multicast service activation at the GGSN.
- Reporting of successful user specific MBMS multicast service activation by GGSN to BM-SC to synchronize the BM-SC UE MBMS context and charging with the MBMS UE contexts in GGSN.
- Reporting of release or deactivation of user specific MBMS multicast service activation by GGSN to BM-SC to synchronize the BM-SC UE MBMS context and charging with the MBMS UE contexts in GGSN.
- BM-SC initiated deactivation of user specific MBMS bearer service when the MBMS user service is terminated.

### MBMS UE Context

A MBMS UE context is defined per UE. Session Manager assign a separate context structure for a MBMS UE Context.

Session Manager maintains the following information as part of MBMS UE Context:

- IP multicast address: IP multicast address identifying an MBMS bearer that the UE has joined.
- APN: Access Point Name on which this IP multicast address is defined.
- SGSN address: The IP address of SGSN
- IMSI: IMSI identifying the user.
- TEID for Control Plane: The Tunnel Endpoint Identifier for the control plane between SGSN and GGSN.
- MBMS NSAPI: Network layer Service Access Point Identifier which identifies an MBMS UE Context.



**Important:** For capacity and resource purpose one MBMS UE context is equal to one PDP context.

## MBMS Bearer Context

The MBMS bearer context is created in the SGSN and GGSN for each provisioned MBMS service. This is created when the first MS requests for this service or when a downstream node requests it. Once created, an MBMS context can be in two states:

- Active - is the state in which network resources are required for the transfer of MBMS data.
- Standby - is the state in which no network resources are required.

The MBMS Bearer Context contains all information describing a particular MBMS bearer service and is created in each node involved in the delivery of the MBMS data.

## Broadcast Multicast Service Center (BM-SC)

The BM-SC includes functions for MBMS user service provisioning and delivery. It serves as an entry point for content provider MBMS transmissions, used to authorize and initiate MBMS Bearer Services within the PLMN. It can also be used to schedule and deliver MBMS transmissions.

The BM-SC consists of five sub-functions:

- Membership function
- Session and Transmission function
- Proxy and Transport function
- Service Announcement function
- Security function.

BM-SC is a functional entity and must exist for each MBMS User Service.

## How MBMS Works

The Multimedia Broadcast Multicast System provides two types of service provisioning; broadcast and multicast modes. This section describes the procedure of these modes.

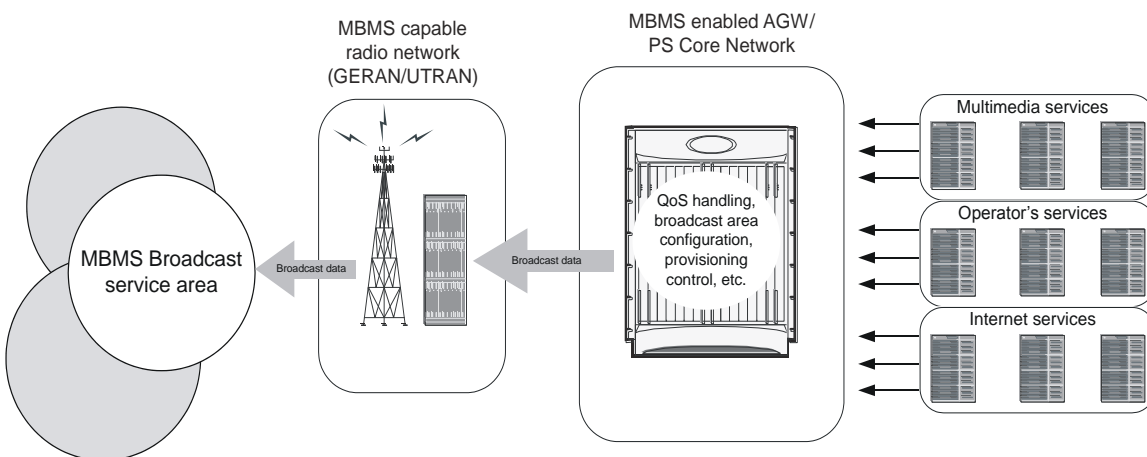
### MBMS Broadcast Mode

The broadcast mode provides unidirectional point-to-multipoint type transmission of multimedia data from a single source to all users that found in a defined broadcast service area. This mode uses radio resources efficiently, since the data is transmitted over a common channel.

MBMS data transmission adapts to the suitable RAN capabilities, depending on the availability of radio resources too. If needed, the bit rate of MBMS data may be varied in order to optimized radio resources.

The following figure shows the basic outline of broadcast mode procedure of an MBMS service in order to broadcast MBMS data within the defined broadcast service area via a packet switched core network.

**Figure 72. Basic Procedure of MBMS Broadcast Mode**



The broadcast service may include one or more successive broadcast sessions. The user can control the enabling or disabling of the MBMS broadcast mode service.

### MBMS Broadcast Mode Procedure

The MBMS performs following steps for broadcast mode user service:

- Step 1** Service Announcement: Through the service announcement mechanisms, like SMS, WAP, users informed about the available MBMS services.
- Step 2** Session Start: This is the phase where BM-SC has data to send and this triggers establishment of network resources for data transfer irrespective of whether a given user has activated the service or not.
- Step 3** MBMS Notification: Notifies the MS of a impending MBMS data transfer.

- Step 4** Data Transfer: It is the phase when MBMS data are transferred to the UEs.
- Step 5** Session Stop: In this phase, the BM-SC determines that it has no more data to send for a time period and so the network resources can be released.

## MBMS Multicast Mode

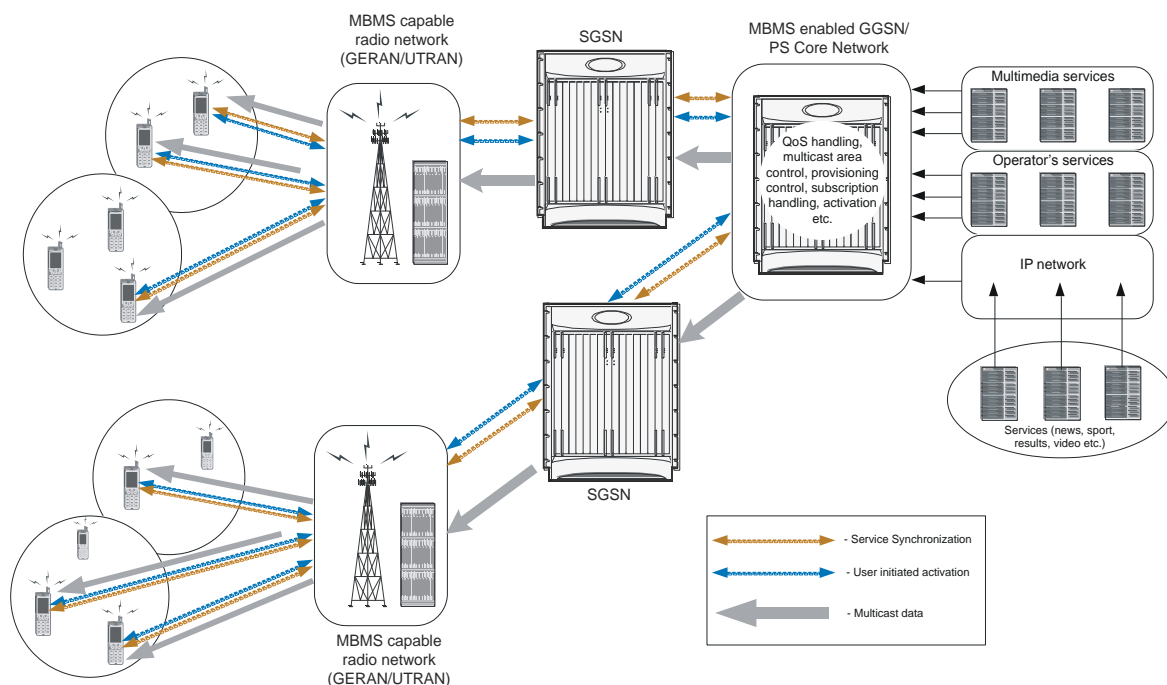
The multicast mode provides unidirectional point-to-multipoint type transmission of multimedia data from a single content source to a group of subscribers that subscribed to specific multicast service separately. The basic difference between broadcast and multicast modes is that the user does not need to subscribe in each broadcast service separately, whereas in multicast mode the services can be ordered separately. The subscription and group joining for the multicast mode service can be done by the operator, user, or a separate service provider.

Like broadcast mode the multicast mode allows the unidirectional point-to-multipoint transmission of multimedia data within the multicast service area. The multicast mode uses radio resources in an efficient way by using a common radio channel as in broadcast mode. Data is transmitted over the multicast service area as defined by the network operator.

The multicast mode provides the flexibility for the network to selectively transmit to those cells within the multicast service area that contains members of a multicast group.

The following figure shows the basic outline of multicast mode procedure of an MBMS service in order to multicast MBMS data within the defined multicast service area via a packet switched core network.

**Figure 73. Basic Procedure of MBMS Multicast Mode**



A multicast service might consist of a single on-going session or may include several simultaneous multicast sessions over an extended period of time.

Some examples of multicast mode service are:

- transmission of sports video clips to subscribers on a charging basis

- transmission of news, movie, song, and audio clips to subscribed users on charging basis

## MBMS Multicast Mode Procedure

The MBMS performs following steps for multicast mode user service:

- Step 1** Subscription: Establishes the relationship between the user and the service provider, which allows the user to receive the related MBMS multicast service.
- Step 2** Service Announcement: Through the service announcement mechanisms like, SMS, WAP, users shall be informed about the available MBMS services.
- Step 3** Joining: This is the process by which a subscriber joins a multicast group, i.e. the user indicates to the network that he/she wants to receive Multicast mode data of a specific MBMS bearer service.
- Step 4** Session Start: This is the phase where BM-SC is ready to send data and this triggers establishment of network resources for data transfer irrespective of whether a given user has activated the service or not.
- Step 5** MBMS Notification: Notifies the MS of a impending MBMS data transfer.
- Step 6** Data Transfer: It is the phase when MBMS data are transferred to the UEs.
- Step 7** Session Stop: In this phase, the BM-SC determines that it has no more data to send for a time period and so the network resources can be released.
- Step 8** Leaving: In this phase, the user leaves a MBMS group through an Internet Group Management Protocol (IGMP) Leave message.

## MBMS Configuration

This section provides a high-level series of steps and the associated configuration examples for configuring the system with MBMS user service in GGSN services.



**Important:** These instructions assume that you have already configured the GGSN/SGSN system level configuration as described in network function *Administration Guide*.

To configure the system to perform Multimedia Broadcast and Multicast service:

- Step 1** Configure the BM-SC profile in a context by applying the example configurations presented in the *BMSC Profile Configuration* section.
- Step 2** Configure the MBMS charging parameters in GTPP Server Group Configuration mode by applying the example configurations presented in the *MBMS GTPP Configuration* section.
- Step 3** Configure the MBMS accounting, supported contexts, timeout parameters, and BMSC profile association with APN in APN configuration mode by applying the example configurations presented in the *MBMS APN Configuration* section.
- Step 4** Enable the MBMS user service provisioning mode in GGSN and configure the number of MBMS UE and MBMS bearer context in GGSN configuration mode by applying the example configurations presented in the *MBMS Provisioning* section.
- Step 5** Save the changes to system configuration by applying the example configuration found in *Verifying and Saving Your Configuration* chapter.
- Step 6** Verify configuration of MBMS service related parameters by applying the commands provided in the *Managing Your Configuration* section of this chapter.

## BMSC Profile Configuration

This section provides the configuration example to configure the BM-SC profile in a context:

```
configure

context <vpn_context_name> [ -noconfirm ]

    bmsc-profile name <profile_name> [ -noconfirm ]

        default gmb diameter dictionary

        gmb diameter endpoint <endpoint_name>

        gmb diameter peer-select peer <peer_name> [ realm <realm_name> ] [ secondary-
peer <sec_peer_name> [ realm <sec_realm_name> ]]

        default gmb user-data mode-preference

    end
```

## MBMS GTPP Configuration

This section provides the configuration example to configure the GTPP server parameters in GTPP group configuration mode for MBMS charging:

```
configure
```

```
context <vpn_context_name> [ -noconfirm ]

  gtp group default

    gtp mbms buckets <cc_bucket>

    gtp mbms interval <duration_sec>

    gtp mbms tariff time1 <mins> <hours> [ time2 <mins> <hours> ]

    gtp mbms volume <download_bytes>

  end
```

## MBMS APN Configuration

This section provides the configuration example to enable the BM-SC profile for an APN and to configure the MBMS accounting, supported contexts, and timeout parameters in APN configuration mode:

```
configure
```

```
context <vpn_context_name>

  apn <apn_name> [ -noconfirm ]

    mbms bmsc-profile name <profile_name>

    default max-contexts

    accounting mode gtp

    default mbms bearer timeout { absolute | idle }

    default mbms ue timeout absolute

  end
```

## MBMS Provisioning

This section provides the configuration example for provisioning of MBMS service mode for a GGSN service and associating the MBMS policy for multicast broadcast within the GGSN service in GGSN service configuration mode:

```
configure
```

```
context <vpn_context_name>
```



```
ggsn-service <ggsn_service_name>  
  
    mbms policy multicast broadcast  
  
end
```

## Save the Configuration

To save changes made to the system configuration for this service, refer *Verifying and Saving Your Configuration* chapter.

# Managing Your Configuration

This section explains how to display and review the configurations after saving them in a *.cfg* file as described in *Saving Your Configuration* chapter of this guide and also to retrieve errors and warnings within an active configuration for a service.



**Important:** All commands listed here are under Exec mode. Not all commands are available on all platforms.

Output descriptions for most of the commands are located in *Command Line Interface Reference*.

To do this:	Enter this command:
<b>View Administrative Information</b>	
Display Current Administrative User Access	
View a list of all administrative users currently logged on to the system	<code>show administrators</code>
View the context in which the administrative user is working, the IP address from which the administrative user is accessing the CLI, and a system generated ID number	<code>show administrators session id</code>
View information pertaining to local-user administrative accounts configured for the system	<code>show local-user verbose</code>
View statistics for local-user administrative accounts	<code>show local-user statistics verbose</code>
View information pertaining to your CLI session	<code>show cli</code>
Determining the System's Uptime	
View the system's uptime (time since last reboot)	<code>show system uptime</code>
View the Status of Configured NTP Servers	
View the status of the configured NTP servers	<code>show ntp status</code>
View the Statistics of Broadcast Multicast service	
View the full information of all broadcast-multicast service session	<code>show multicast-sessions full all</code>
View the status of all broadcast multicast-service session	<code>show session in-progress</code>
View all session for broadcast-multicast service	<code>show multicast-sessions all</code>
View Subscribers Currently Accessing the System	
View a listing of subscribers currently accessing the system	<code>show subscribers all</code>
View information for a specific subscriber	<code>show subscribers full username &lt;user_name&gt;</code>
<b>View the MBMS Related Information</b>	
Display Configured MBMS service	
View the configuration of a context	<code>show configuration context &lt;vpn_ctxt_name&gt;</code>

To do this:	Enter this command:
View configuration errors for GGSN service	<code>show configuration errors section ggsn-service [ verbose ] [   {grep &lt;grep_options&gt;   more } ]</code>
Display BM-SC server Information	<code>show bmsc servers</code>

## Gathering MBMS Statistics

The following table lists the commands that can be used to gather the statistics for MBMS.



**Important:** All commands listed here are under Exec mode. For more information on these commands, refer *Executive Mode Commands* chapter in *Command Line Interface Reference*.

Table 35. Gathering Statistics

Statistics Wanted	Action to Perform	Information to Look For
Gmb interface statistics for APN and BM-SC profile	At the Exec Mode prompt, enter the following command:  <pre>show gmb statistics [ apn &lt;apn_name&gt;   bmsc-profile &lt;bmsc_profile_name&gt; ] [ verbose ]</pre>	The output of this command displays the statistics about the Gmb interface session for MBMS on an APN.
Detailed MBMS bearer service statistics	At the Exec Mode prompt, enter the following command:  <pre>show mbms bearer-service [ mcast-address &lt;mcast_address&gt; ] [ apn &lt;apn_name&gt; ] [ bmsc-profile &lt;bmsc_profile_name&gt; ] [ service-type { multicast   broadcast } ] [ summary   full ] [ all ]</pre>	The output of this command displays the MBMS bearer service statistics.
Detailed statistics of MBMS multicast sessions	At the Exec Mode prompt, enter the following command:  <pre>show multicast-sessions</pre>	The output of this command displays the detailed statistics of MBMS multicast session running on system.



# Appendix M

## Multi-Protocol Label Switching (MPLS) Support

---

This chapter describes the system's support for BGP/MPLS VPN and explains how it is configured. The product administration guides provide examples and procedures for configuration of basic services on specific systems. It is recommended that you select the configuration example that best meets your service model and configure the required elements for that model, as described in the respective product administration guide, before using the procedures in this chapter.

When enabled through a feature license key, the system supports MPLS to provide a VPN connectivity from the system to the corporate's network.



**Important:** This release provides BGP/MPLS VPN for directly connected PE routers only.

---

MP-BGP is used to negotiate the routes and segregate the traffic for the VPNs. The network node learns the VPN routes from the connected Provider Edge (PE), while the PE populates its routing table with the routes provided by the network functions.

This chapter includes following sections:

- [Overview](#)
- [Supported Standards](#)
- [Supported Networks and Platforms](#)
- [Licenses](#)
- [Benefits](#)
- [Configuring BGP/MPLS VPN with Static Labels](#)
- [Configuring BGP/MPLS VPN with Dynamic Labels](#)

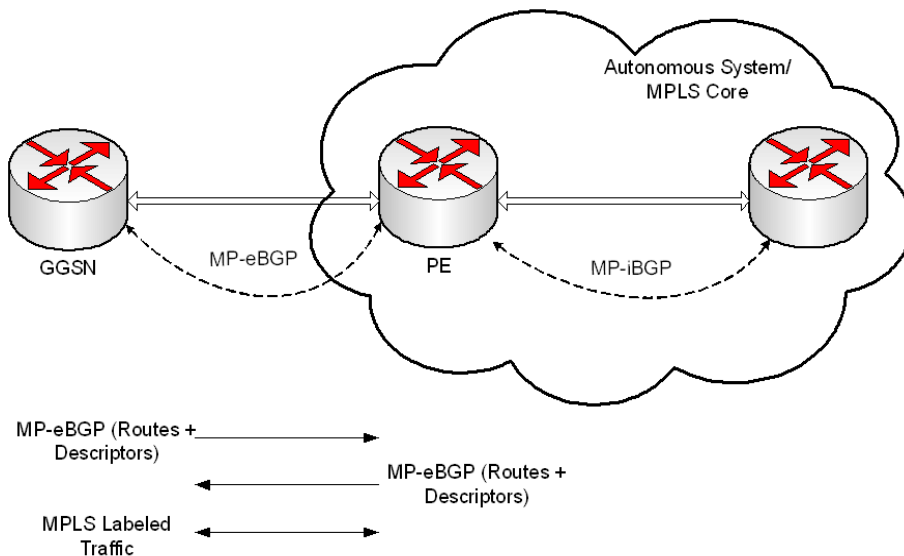
## Overview

As seen in the following scenario, the chassis can be deployed as a router while supporting BGP/MPLS-VPN in a network.

- Chassis as MPLS-Customer Edge (MPLS-CE) connecting to Provider Edge (PE)
- Chassis as MPLS-Customer Edge (MPLS-CE) connecting to Autonomous System Border Router (ASBR)

## Chassis as MPLS-CE Connecting to PE

Figure 74. Chassis as MPLS-CE Connected to PE



The system in this scenario uses static/dynamic MPLS labels for ingress and egress traffic. For configuration information on static label, refer to the [Configuring BGP/MPLS VPN with Static Labels](#) section and refer [Configuring BGP/MPLS VPN with Dynamic Labels](#) for dynamic label configuration.

The system is in a separate autonomous system (AS) from the Provider Edge (PE). It communicates with the PE and all VPN routes are exchanged over MP-BGP. Routes belonging to different VPNs are logically separated, using separate virtual route forwarding tables (VRFs).

Routes for each VPN are advertised as VPN-IPv4 routes, where route distinguishers are prepended to regular IPv4 routes to allow them to be unique within the routing table. Route targets added to the BGP extended community attributes identify different VPN address spaces. The particular upstream BGP peer routing domain (VPN), from which a route is to be imported by the downstream peer into an appropriate VRF, is identified with an extended community in the advertised NLRI.

A unique label is also received or advertised for every VPN route.

The Customer Edge (CE) also advertises routes to the PE using NLRIs that include route distinguishers to differentiate VPNs, an extended community to identify VRFs, and a MPLS-label, which will later be used to forward data traffic.



There is a single MPLS-capable link between the CE and the PE. MP-BGP communicates across this link as a TCP session over IP. Data packets are sent bidirectionally as MPLS encapsulated packets.

This solution does not use any MPLS protocols. The MPLS label corresponding to the immediate upstream neighbor can be statically configured on the downstream router, and similarly in the reverse direction.

When forwarding subscriber packets in the upstream direction to the PE, the CE encapsulates packets with MPLS headers that identify the upstream VRF (the label sent with the NLRI) and the immediate next hop. When the PE receives a packet it swaps the label and forward.

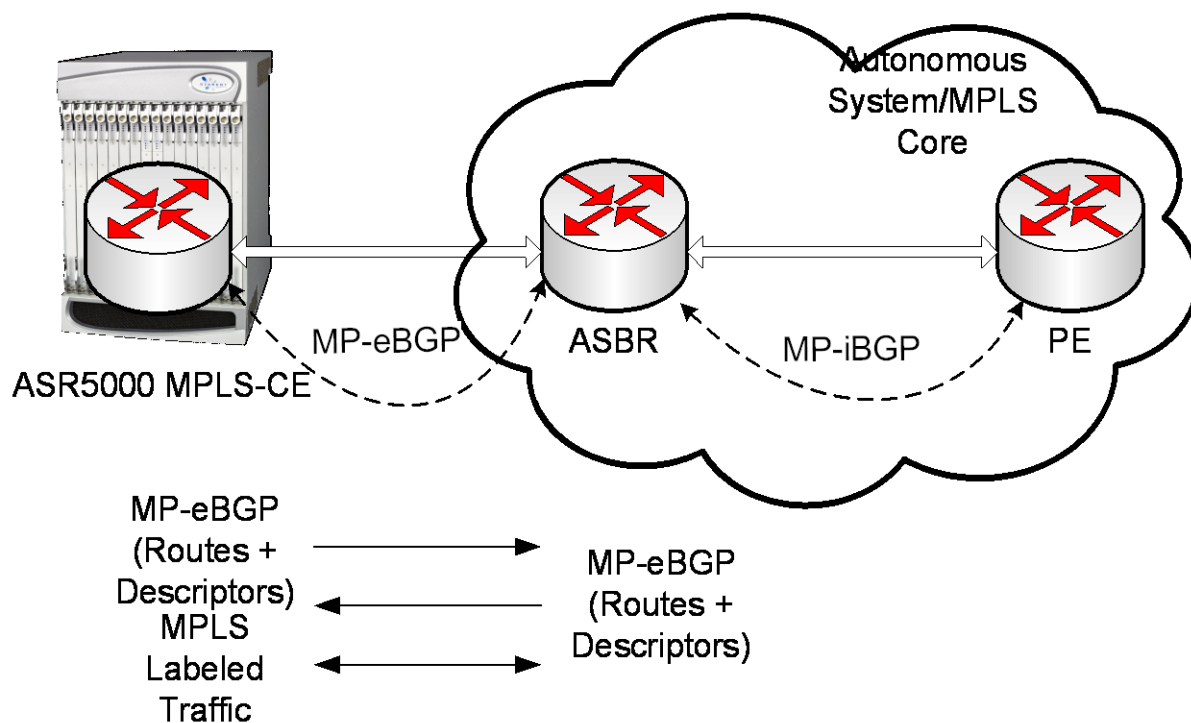
The CE does not run any MPLS protocol (LDP or RSVP-TE).

When receiving data packets in the downstream direction from the PE, the label is checked to identify the destination VRF. Then the packet is de-encapsulated into an IP packet and sent to the session subsystem for processing.

**Important:** MPLS ping/trace route debugging facilities are not supported.

## Chassis as MPLS-CE Connected to ASBR

Figure 75. Chassis as MPLS-CE Connected to ASBR



The system in this scenario uses static/dynamic MPLS labels for ingress and egress traffic. For configuration information on static label, refer to the [Configuring BGP/MPLS VPN with Static Labels](#) section and refer [Configuring BGP/MPLS VPN with Dynamic Labels](#) for dynamic label configuration.

This scenario differs from the MPLS-CE with PE scenario in terms of peer functionality even though MPLS-CE functionality does not change. Like the MPLS-CE with PE scenario, MPLS-CE system maintains VRF routes in various VRFs and exchanges route information with peer over MP-eBGP session.

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

## Engineering Rules

- Up to 250 virtual routing tables per context.
- Up to 5000 “host routes” spread across multiple VRFs per BGP process. Limited to 6000 pool routes per chassis.
- Up to 1024 VRFs per chassis.

## Supported Standards

Support for the following standards and requests for comments (RFCs) have been added with this interface support:

- RFC 4364, BGP/MPLS IP VPNs
- RFC 3032, MPLS Label Stack Encoding



**Important:** One or more sections of above mentioned IETF are partially supported for this feature. For more information on Statement of Compliance, contact your Cisco account representative.

---

## Supported Networks and Platforms

This feature supports all ASR5x00 platforms with StarOS Release 9.0 or later running with network function services.

# Licenses

Multi-protocol label switching (MPLS) is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

## Benefits


MPLS provides networks with a more efficient way to manage applications and move information between locations. MPLS prioritizes network traffic, so administrators can specify which applications should move across the network ahead of others.


## Configuring BGP/MPLS VPN with Static Labels

This section describes the procedures required to configure the system as an MPLS-CE to interact with a PE with static MPLS label support.

The base configuration, as described in the *Routing* chapter in this guide, must be completed prior to attempt the configuration procedure described below.

---

 **Important:** The feature described in this chapter is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements.

 **Important:** Commands used in the configuration samples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the *Command Line Interface Reference* for complete information regarding all commands.

---

To configure the system for BGP/MPLS VPN:

- Step 1** Create a VRF on the router and assign a VRF name by applying the example configuration in the *Create VRF with Route-distinguisher and Route-target* section.
- Step 2** Set the neighbors and address family to exchange routing information and establish BGP peering with a peer router by applying the example configuration in the *Set Neighbors and Enable VPNv4 Route Exchange* section.
- Step 3** Configure the address family and redistribute the connected routes domains into BGP by applying the example configuration in the *Configure Address Family and Redistribute Connected Routes* section. This takes any routes from another protocol and redistributes them to BGP neighbors using the BGP protocol.
- Step 4** Configure IP Pools with MPLS labels for input and output by applying the example configuration in the *Configure IP Pools with MPLS Labels* section.
- Step 5** *Optional.* Bind DHCP service to work with MPLS labels for input and output in corporate networks by applying the example configuration in the *Bind DHCP Service for Corporate Servers* section.
- Step 6** *Optional.* Bind AAA/RADIUS server group in corporate network to work with MPLS labels for input and output by applying the example configuration in the *Bind AAA Group for Corporate Servers* section.
- Step 7** Save your configuration as described in the *System Administration Guide*.

### Create VRF with Route-distinguisher and Route-target

Use this example to first create a VRF on the router and assign a VRF name. The second **ip vrf** command creates the route-distinguisher and route-target.

```
configure

context <context_name> -noconfirm

ip vrf <vrf_name>
```

```

router bgp <as_number>

  ip vrf <vrf_name>

    route-distinguisher {<as_value> | <ip_address>} <rt_value>

    route-target export {<as_value> | <ip_address>} <rt_value>

  end

```

## Set Neighbors and Enable VPNv4 Route Exchange

Use this example to set the neighbors and address family to exchange VPNv4 routing information with a peer router.

**configure**

```

context <context_name>

  router bgp <as_number>

    neighbor <ip_address> remote-as <AS_num>

    address-family vpnv4

    neighbor <ip_address> activate

    neighbor <ip_address> send-community both

  exit

  interface <bind_intf_name>

    ip address <ip_addr_mask_combo>

  end

```

## Configure Address Family and Redistributed Connected Routes

Use this example to configure the **address-family** and to **redistribute** the connected routes or IP pools into BGP. This takes any routes from another protocol and redistributes them using the BGP protocol.

**configure**

```

context <context_name>

  router bgp <as_number>

    address-family ipv4 <type> vrf <vrf_name>

      redistribute connected

    end

```



## Configure IP Pools with MPLS Labels

Use this example to configure IP Pools with MPLS labels for input and output.

```
configure

context <context_name> -noconfirm

    ip pool <name> <ip_addr_mask_combo> private vrf <vrf_name> mpls-label input
    <in_label_value> output <out_label_value1> nexthop-forwarding-address
    <ip_addr_bgp_neighbor>

end
```

## Bind DHCP Service for Corporate Servers

Use this example to bind DHCP service with MPLS labels for input and output in Corporate network.

```
configure

context <dest_ctxt_name>

    interface <intfc_name> loopback

        ip vrf forwarding <vrf_name>

        ip address <bind_ip_address subnet_mask>

    exit

    dhcp-service <dhcp_svc_name>

        dhcp ip vrf <vrf_name>

        bind address <bind_ip_address> [ nexthop-forwarding-address
        <nexthop_ip_address> [ mpls-label input <in_mpls_label_value> output
        <out_mpls_label_value1> [ <out_mpls_label_value2> ]]]

        dhcp server <ip_address>

    end
```

Notes:

- To ensure proper operation, DHCP functionality should be configured within a destination context.
- Optional keyword **nexthop-forwarding-address** <ip\_address> **mpls-label input** <in\_mpls\_label\_value> **output** <out\_mpls\_label\_value1> applies DHCP over MPLS traffic.

## Bind AAA Group for Corporate Servers

Use this example to bind AAA server groups with MPLS labels for input and output in Corporate network.

```

configure

context <dest_ctxt_name>

    aaa group <aaa_grp_name>

        radius ip vrf <vrf_name>

        radius attribute nas-ip-address address <nas_address> nexthop-forwarding-
address <ip_address> mpls-label input <in_mpls_label_value> output <
<out_mpls_label_value1>

        radius server <ip_address> encrypted key <encrypt_string> port
<iport_num>

    end

```

## Notes:


- *aaa\_grp\_name* is a pre-configured AAA server group configured in Context Configuration mode. Refer *AAA Interface Administration Reference* for more information on AAA group configuration.
- Optional keyword **nexthop-forwarding-address** <ip\_address> **mpls-label input** <in\_mpls\_label\_value> **output** <out\_mpls\_label\_value1> associates AAA group for MPLS traffic.


## Configuring BGP/MPLS VPN with Dynamic Labels

This section describes the procedures required to configure the system as an MPLS-CE to interact with a PE with dynamic MPLS label support.

The base configuration, as described in the *Routing* chapter in this guide, must be completed prior to attempt the configuration procedure described below.

---

 **Important:** The features described in this chapter is an enhanced feature and need enhanced feature license. This support is only available if you have purchased and installed particular feature support license on your chassis.

 **Important:** Commands used in the configuration samples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the *Command Line Interface Reference* for complete information regarding all commands.

---

To configure the system for BGP/MPLS VPN:

- Step 1** Create a VRF on the router and assign a VRF name by applying the example configuration in the *Create VRF with Route-distinguisher and Route-target* section.
- Step 2** Set the neighbors and address family to exchange routing information and establish BGP peering with a peer router by applying the example configuration in the *Set Neighbors and Enable VPNv4 Route Exchange* section.
- Step 3** Configure the address family and redistribute the connected routes domains into BGP by applying the example configuration in the *Configure Address Family and Redistribute Connected Routes* section. This takes any routes from another protocol and redistributes them to BGP neighbors using the BGP protocol.
- Step 4** Configure IP Pools with dynamic MPLS labels by applying the example configuration in the [Configure IP Pools with MPLS Labels](#) section.
- Step 5** *Optional.* Bind DHCP service to work with dynamic MPLS labels in corporate networks by applying the example configuration in the *Bind DHCP Service for Corporate Servers* section.
- Step 6** *Optional.* Bind AAA/RADIUS server group in corporate network to work with dynamic MPLS labels by applying the example configuration in the *Bind AAA Group for Corporate Servers* section.
- Step 7** *Optional.* Modify the configured IP VRF, which is configured to support basic MPLS functionality, for mapping between DSCP bit value and experimental (EXP) bit value in MPLS header for ingress and egress traffic by applying the example configuration in the *DSCP and EXP Bit Mapping* section.
- Step 8** Save your configuration as described in the *System Administration Guide*.

### Create VRF with Route-distinguisher and Route-target

Use this example to first create a VRF on the router and assign a VRF name. The second `ip vrf` command creates the route-distinguisher and route-target.

```
configure
```

```

context <context_name> -noconfirm

  ip vrf <vrf_name>

  router bgp <as_number>

    ip vrf <vrf_name>

      route-distinguisher {<as_value> | <ip_address>} <rt_value>

      route-target export {<as_value> | <ip_address>} <rt_value>

      route-target import {<as_value> | <ip_address>} <rt_value>

    end

```

Notes:

- If export and import route targets are the same, alternate command **route-target both** {<as\_value> | <ip\_address>} <rt\_value> can be used in place of **route-target import** and **route-target export** commands.

## Set Neighbors and Enable VPNv4 Route Exchange

Use this example to set the neighbors and address family to exchange VPNv4 routing information with a peer router.

**configure**

```

context <context_name>

  mpls bgp forwarding

  router bgp <as_number>

    neighbor <ip_address> remote-as <AS_num>

    address-family vpnv4

      neighbor <ip_address> activate

      neighbor <ip_address> send-community both

    exit

  interface <bind_intf_name>

    ip address <ip_addr_mask_combo>

  end

```

## Configure Address Family and Redistributed Connected Routes

Use this example to configure the **address-family** and to **redistribute** the connected routes or IP pools into BGP. This takes any routes from another protocol and redistributes them using the BGP protocol.

```
configure

context <context_name>

  router bgp <as_number>

    address-family ipv4 <type> vrf <vrf_name>

      redistribute connected

    end
```

## Configure IP Pools with MPLS Labels

Use this example to configure IP Pools with dynamic MPLS labels.

```
configure

context <context_name> -noconfirm

  ip pool <name> <ip_addr_mask_combo> private vrf <vrf_name>

end
```

## Bind DHCP Service for Corporate Servers

Use this example to bind DHCP service with dynamic MPLS labels in Corporate network.

```
configure

context <dest_ctxt_name>

  interface <intfc_name> loopback

    ip vrf forwarding <vrf_name>

    ip address <bind_ip_address subnet_mask>

  exit

  dhcp-service <dhcp_svc_name>

    dhcp ip vrf <vrf_name>

    bind address <bind_ip_address>

    dhcp server <ip_address>
```

```
end
```

Notes:

- To ensure proper operation, DHCP functionality should be configured within a destination context.

## Bind AAA Group for Corporate Servers

Use this example to bind AAA server groups with dynamic MPLS labels in Corporate network.

```
configure

context <dest_ctxt_name>

  aaa group <aaa_grp_name>

    radius ip vrf <vrf_name>

    radius attribute nas-ip-address address <nas_address>

    radius server <ip_address> encrypted key <encrypt_string> port
<iport_num>

  end
```

Notes:

- *aaa\_grp\_name* is a pre-configured AAA server group configured in Context Configuration mode. Refer *AAA Interface Administration Reference* for more information on AAA group configuration.

## DSCP and EXP Bit Mapping

Use this example to modify the configured IP VRF to support QoS mapping.

```
configure

context <context_name>

  ip vrf <vrf_name>

    mpls map-dscp-to-exp dscp <dscp_bit_value> exp <exp_bit_value>

    mpls map-exp-to-dscp exp <exp_bit_value> dscp <dscp_bit_value>

  end
```

# Appendix N

## Rejection/Redirection of HA Sessions on Network Failures

---

This chapter provides information on configuring an enhanced, or extended, service. The product Administration Guides provide examples and procedures for configuration of basic services on the system. It is recommended that you select the configuration example that best meets your service model, and configure the required elements for that model, as described in the respective product Administration Guide, before using the procedures in this chapter.

The following sections are included in this chapter:

- [Overview](#)
- [Configuring HA Session Redirection](#)
- [RADIUS Attributes](#)

# Overview

This feature enables the HA service to either reject new calls or redirect them to another HA when a destination network connection failure is detected. When network connectivity is re-established, the HA service begins to accept calls again in the normal manner.

The way this is implemented in the system is as follows:

- A policy is configured in the HA service that tells the service what action to take when network connectivity is lost. New calls are either directed to one of up to 16 different IP addresses or all new calls are rejected until network connectivity is restored.
- In the destination context, a network reachability server is configured. This is a device on the destination network to which ping packets are periodically sent to determine if the network is reachable. As soon as a network reachability server is configured, pinging of the server commences whether or not the server name is bound to a subscriber or an IP pool.
- The name of the network reachability server configured in the destination context is bound to either a local subscriber profile or an IP pool. If the subscriber is authenticated by an AAA server, RADIUS attributes may specify the network reachability server for the subscriber. (If an IP pool has a network reachability server name bound to it, that takes precedence over both the RADIUS attributes and the local subscriber configuration.)



## Configuring HA Session Redirection

This section provides instructions for configuring rejection or redirection of HA sessions on the event of a network failure. These instructions assume that there is a destination context, and HA service, an IP pool, and a subscriber already configured and that you are at the root prompt for the Exec mode:

```
[local]host_name#
```

**Step 1** Enter the global configuration mode by entering the following command:

```
configure
```

The following prompt appears:

```
[local]host_name(config)#
```

**Step 2** Enter context configuration mode by entering the following command:

```
context <context_name>
```

*context\_name* is the name of the destination context where the HA service is configured. The name must be from 1 to 63 alpha and/or numeric characters and is case sensitive. The following prompt appears:

```
[<context_name>]host_name(config-ctx)#
```

**Step 3** Enter the HA service configuration mode by entering the following command:

```
ha-service <ha_service_name>
```

*ha\_service\_name* is the name of the HA service. The name must be from 1 to 63 alpha and/or numeric characters and is case sensitive. The following prompt appears:

```
[<context_name>]host_name(config-ha-service)#
```

**Step 4** Configure the action for the HA service to take when network connectivity is lost by entering the following command:

```
policy nw-reachability-fail { reject [ use-reject-code { admin-prohibited |
insufficient-resources } ] | redirect <ip_addr1> [ weight <value> ] [ <ip_addr2>
[ weight <value> ] ] ... [ <ip_addr16> [ weight <value> ] ] }
```

Keyword/Variable	Description
<b>reject</b>	Upon network reachability failure reject all new calls for this context.
<b>use-reject-code { admin-prohibited   insufficient-resources }</b>	When rejecting calls send the specified reject code. If this keyword is not specified the admin-prohibited reject code is sent by default.

Keyword/Variable	Description
<pre> <b>redirect</b> &lt;ip_addr1&gt; [ <b>weight</b> &lt;value&gt; ] [ &lt;ip_addr2&gt; [ <b>weight</b> &lt;value&gt; ] ] ... [ &lt;ip_addr16&gt; [ <b>weight</b> &lt;value&gt; ] ] </pre>	<p>Upon network reachability failure redirect all calls to the specified IP address.</p> <p><b>&lt;ip_addr&gt;</b>: This must be an IPv4 address. Up to 16 IP addresses and optional weight values can be entered on one command line.</p> <p><b>weight &lt;value&gt;</b>: When multiple addresses are specified, they are selected in a weighted round-robin scheme. If a weight is not specified, the entry is automatically assigned a weight of 1.</p> <p><b>&lt;value&gt;</b> must be an integer from 1 through 10.</p>

**Step 5** Enter the following command to return to the context configuration mode:

```
exit
```

The following prompt appears:

```
[<context_name>]host_name(config-ctx)#
```

**Step 6** Specify the network device on the destination network to which ping packets should be sent to test for network reachability, by entering the following command:

```

nw-reachability server <server_name> [ interval <seconds> ] [ local-addr
<ip_addr> ] [ num-retry <num> ] [ remote-addr <ip_addr> ] [ timeout <seconds> ]

```

Keyword/Variable	Description
<i>server_name</i>	A name for the network device that is sent ping packets to test for network reachability.
<b>interval</b> <i>&lt;seconds&gt;</i>	Default: 60 seconds Specifies the frequency in seconds for sending ping requests. <i>&lt;seconds&gt;</i> must be an integer from 1 through 3600.
<b>local-addr</b> <i>&lt;ip_addr&gt;</i>	Specifies the IP address to be used as the source address of the ping packets; If this is unspecified, an arbitrary IP address that is configured in the context is used. <i>&lt;ip_addr&gt;</i> must be an IP v4 address.
<b>num-retry</b> <i>&lt;num&gt;</i>	Default: 5 Specifies the number of retries before deciding that there is a network-failure. <i>&lt;num&gt;</i> must be an integer from 0 through 100.
<b>remote-addr</b> <i>&lt;ip_addr&gt;</i>	Specifies the IP address of a network element to use as the destination to send the ping packets for detecting network failure or reachability. <i>&lt;ip_addr&gt;</i> must be an IPv4 address.
<b>timeout</b> <i>&lt;seconds&gt;</i>	Default: 3 seconds Specifies how long to wait, in seconds, before retransmitting a ping request to the remote address. <i>&lt;seconds&gt;</i> must be an integer from 1 through 10.

- Step 7** Repeat *step 6* to configure additional network reachability servers.
- Step 8** To bind a network reachability server to an IP pool, continue with *step 9*. To bind a network reachability server to a local subscriber profile, skip to *step 11*.
- Step 9** To bind a network reachability server name to an IP pool, enter the following command:

```
ip pool <pool_name> nw-reachability server <server_name>
```

<code>&lt;pool_name&gt;</code>	The name of an existing IP pool in the current context.
<code>nw-reachability server &lt;server_name&gt;</code>	Bind the name of a configured network reachability server to the IP pool and enable network reachability detection for the IP pool. This takes precedence over any network reachability server settings in a subscriber configuration or RADIUS attribute. <code>&lt;server_name&gt;</code> : The name of a network reachability server that has been defined in the current context. This is a string of from 1 through 16 characters.

- Step 10** Repeat *step 9* for additional IP pools in the current context then skip to *step 13*.

- Step 11** Enter the subscriber configuration mode by entering the following command:

```
subscriber { default | name <subs_name> }
```

Where **default** is the default subscriber for the current context and *subs\_name* is the name of the subscriber profile that you want to configure for network reachability. The following prompt appears:

```
[<context_name>]host_name(config-subscriber)#
```

- Step 12** To bind a network reachability server name to the current subscriber in the current context, enter the following command:

```
nw-reachability server <server_name>
```

Where *server\_name* is the name of a network reachability server that has been defined in the current context.

- Step 13** Return to the executive mode by entering the following command:

```
end
```

The following prompt appears:

```
[local]host_name#
```

- Step 14** Enter the executive mode for the destination context for which you configured network reachability by entering the following command:

```
context <context_name>
```

Where *context\_name* is the name of the destination context for which you configured network reachability. The following prompt appears:

```
[context_name]host_name#
```

**Step 15** Check the network reachability server configuration by entering the following command

```
show nw-reachability server all
```

The output of this command appears similar to the following:

```
Server remote-addr local-addr state
-----
nw-server1 192.168.100.20 192.168.1.10 Down

Total Network Reachability Servers: 1 Up: 0
```

Ensure that the remote and local addresses are correct. The state column indicates whether or not the server is reachable (Up) or unreachable (Down).

**Step 16** Check the HA service policy by entering the following command:

```
show ha-service name <ha_service_name>
```

Where *<ha\_service\_name>* is the name of the HA service in the current context for which you configured a network reachability policy. The output of this command includes information about the network reachability policy that looks similar to the following:

```
NW-Reachability Policy: Reject (Reject code: Admin Prohibited)
```

**Step 17** Check the network reachability server name bound to an IP pool by entering the following command:

```
show ip pool pool-name <pool_name>
```

Where *<pool\_name>* is the name of the IP pool to which you bound a network reachability server name. The output of this command includes information about the network reachability server name that looks similar to the following:

```
Network Reachability Detection Server: nw-server1
```

**Step 18** Check the network reachability server name bound to a local subscriber profile by entering the following command:

```
show subscribers configuration username <subscriber_name>
```

Where *<subscriber\_name>* is the name of the local subscriber to which you bound a network reachability server name. The output of this command includes information about the network reachability server name that looks similar to the following:

```
network reachability detection server name: nw-server1
```

**Step 19** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

## RADIUS Attributes

Attributes defined in a subscriber profile stored remotely on a RADIUS server can be used to bind the network reachability server to a subscriber session. Use the following attributes to bind a network reachability server to a subscriber session;

- **SN-Nw-Reachability-Server-Name**
- **SN1-Nw-Reachability-Server-Name**

The attributes have one possible value, which is a variable that is a string of from 1 to 15 characters in length. This should be the name of the configured network reachability server.

The **SN-Nw-Reachability-Server-Name** attribute is contained in the following dictionaries:

- starent
- starent-835

The **SN1-Nw-Reachability-Server-Name** attribute is contained in the following dictionaries:

- starent-vsai
- starent-vsai-835

Refer to the *AAA Interface Administration and Reference* for more details.



# Appendix O

## Policy Forwarding

---

This chapter provides information on configuring an enhanced, or extended, service. The product administration guides provide examples and procedures for configuration of basic services on the system. It is recommended that you select the configuration example that best meets your service model and configure the required elements for that model before using the procedures in this chapter.

Sections in this chapter include:

- [Overview](#)
- [IP Pool-based Next Hop Forwarding](#)
- [Subscriber-based Next Hop Forwarding](#)
- [ACL-based Policy Forwarding](#)

## Overview

The system can be configured to automatically forward data packets to a predetermined network destination. This can be done in one of three ways:

- IP Pool-based Next Hop Forwarding - Forwards data packets based on the IP pool from which a subscriber obtains an IP address.
- ACL-based Policy Forwarding - Forwards data packets based on policies defined in Access Control Lists (ACLs) and applied to contexts or interfaces.
- Subscriber specific Next Hop Forwarding - Forwards all packets for a specific subscriber.

The simplest way to forward subscriber data is to use IP Pool-based Next Hop Forwarding. An IP pool is configured with the address of a next hop gateway and data packets from all subscribers using the IP pool are forward to that gateway.

Subscriber Next Hop forwarding is also very simple. In the subscriber configuration a nexthop forwarding address is specified and all data packets for that subscriber are forwarded to the specified nexthop destination.

ACL-based Policy Forwarding gives you more control on redirecting data packets. By configuring an Access Control List (ACL) you can forward data packets from a context or an interface by different criteria, such as; source or destination IP address, ICMP type, or TCP/UDP port numbers.

ACLs are applied first. If ACL-based Policy Forwarding and Pool-based Next Hop Forwarding or Subscriber are configured, data packets are first redirected as defined in the ACL, then all remaining data packets are redirected to the next hop gateway defined by the IP pool or subscriber profile.



## IP Pool-based Next Hop Forwarding

When an IP pool in a destination context has a Next Hop Forwarding address specified, any subscriber that obtains an IP address from that IP pool has all data coming from the mobile node automatically forwarded to the specified Next Hop Forwarding address.

For more information on creating IP pools, refer to the *System Administration Guide* and for additional information on the `ip pool` command, refer to the *Command Line Interface Reference*.

## Configuring IP Pool-based Next Hop Forwarding

Configure Next Hop Forwarding on an existing IP Pool in a destination context by applying the following example configuration:

```
configure

context <context_name>

    ip pool <pool_name> nexthop-forwarding-address <forwarding_ip_address>

end
```

Save the configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

## Subscriber-based Next Hop Forwarding

When a subscriber configuration has a Next Hop Forwarding address specified, any sessions authenticated as that subscriber have all data coming from the mobile node automatically forwarded to the specified Next Hop Forwarding address.

### Configuring Subscriber-based Next Hop Forwarding

Configure Next Hop Forwarding for a specific subscriber by applying the following example configuration:

```
configure

  context <context_name>

    subscriber name <subs_name>

      nexthop-forwarding-address <forwarding_ip_address>

    end
```

Save the configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

# ACL-based Policy Forwarding

ACL-based Policy Forwarding is a feature in the system that forwards subscriber data based on policies defined in Access Control Lists (ACLs). When ACLs are applied to access groups, priorities are given to the ACLs. The ACL applied with the highest priority is used to define the policy that is used for forwarding the subscriber data.



**Important:** Refer to *Access Control Lists* for additional information on creating and using ACLs.

## Configuring ACL-based Policy Forwarding

Configure ACL-based Policy Forwarding by applying the following example configuration:

```
configure

context <context_name>

    ip access-list <acl_name>

        redirect <interface_name> <next_hop_address> <criteria>

    exit
```

The following example specifies that any IP packet coming from any system on the 192.168.55.0 network that has a destination host address of 192.168.80.1 is to be redirected, or forwarded, through the system interface named *interface2* to the host at 192.168.23.12:

```
redirect interface2 192.168.23.12 ip 192.168.55.0 255.255.255.0 host 192.168.80.1
```

Save the configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

## Applying the ACL to an IP Access Group

To apply the ACL to the IP access group for the current destination context, go to *Applying the ACL to a Destination Context*.

To apply the ACL to the IP access group for an interface in the current destination context, go to [Applying the ACL to an Interface in a Destination Context](#).

## Applying the ACL to a Destination Context

**Step 1** At the context configuration mode prompt, enter the following command:

```
ip access-group <acl_name> {in | out} <priority-value>
```

- Step 2** Save the configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

## Applying the ACL to an Interface in a Destination Context

- Step 1** Set parameters for inbound data by applying the following example configuration:

```
configure
  context <context_name>
    interface <interface_name>
      ip access-group <acl_name> in <priority-value>
    end
```

- Step 2** Set parameters for outbound data by applying the following example configuration:

```
configure
  context <context_name>
    interface <interface_name>
      ip access-group <acl_name> out <priority-value>
    end
```

- Step 3** Save the configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

# Appendix P

## Proxy-Mobile IP

---

This chapter describes system support for Proxy Mobile IP and explains how it is configured. The product administration guides provide examples and procedures for configuration of basic services on the system. It is recommended that you select the configuration example that best meets your service model before using the procedures in this chapter.


Proxy Mobile IP provides a mobility solution for subscribers with mobile nodes (MNs) capable of supporting only Simple IP.

This chapter includes the following sections:

- [Overview](#)
- [How Proxy Mobile IP Works in 3GPP2 Network](#)
- [How Proxy Mobile IP Works in 3GPP Network](#)
- [How Proxy Mobile IP Works in WiMAX Network](#)
- [How Proxy Mobile IP Works in a WiFi Network with Multiple Authentication](#)
- [Configuring Proxy Mobile-IP Support](#)

# Overview

Proxy Mobile IP provides mobility for subscribers with MNs that do not support the Mobile IP protocol stack.

 **Important:** Proxy Mobile IP is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

The Proxy Mobile IP feature is supported for various products. The following table indicates the products on which the feature is supported and the relevant sections within the chapter that pertain to that product.

**Table 36. Applicable Products and Relevant Sections**

Applicable Product(s)	Refer to Sections
PDSN	<ul style="list-style-type: none"> <li>• <a href="#">Proxy Mobile IP in 3GPP2 Service</a></li> <li>• <a href="#">How Proxy Mobile IP Works in 3GPP2 Network</a></li> <li>• <a href="#">Configuring FA Services</a></li> <li>• <a href="#">Configuring Proxy MIP HA Failover</a></li> <li>• <a href="#">Configuring HA Services</a></li> <li>• <a href="#">Configuring Subscriber Profile RADIUS Attributes</a></li> <li>• <a href="#">RADIUS Attributes Required for Proxy Mobile IP</a></li> <li>• <a href="#">Configuring Local Subscriber Profiles for Proxy-MIP on a PDSN</a></li> <li>• <a href="#">Configuring Default Subscriber Parameters in Home Agent Context</a></li> </ul>
GGSN	<ul style="list-style-type: none"> <li>• <a href="#">Proxy Mobile IP in 3GPP Service</a></li> <li>• <a href="#">How Proxy Mobile IP Works in 3GPP Network</a></li> <li>• <a href="#">Configuring FA Services</a></li> <li>• <a href="#">Configuring Proxy MIP HA Failover</a></li> <li>• <a href="#">Configuring HA Services</a></li> <li>• <a href="#">Configuring Subscriber Profile RADIUS Attributes</a></li> <li>• <a href="#">RADIUS Attributes Required for Proxy Mobile IP</a></li> <li>• <a href="#">Configuring Default Subscriber Parameters in Home Agent Context</a></li> <li>• <a href="#">Configuring APN Parameters</a></li> </ul>

Applicable Product(s)	Refer to Sections
ASN GW	<ul style="list-style-type: none"> <li>• <a href="#">Proxy Mobile IP in WiMAX Service</a></li> <li>• <a href="#">How Proxy Mobile IP Works in WiMAX Network</a></li> <li>• <a href="#">Configuring FA Services</a></li> <li>• <a href="#">Configuring Proxy MIP HA Failover</a></li> <li>• <a href="#">Configuring HA Services</a></li> <li>• <a href="#">Configuring Subscriber Profile RADIUS Attributes</a></li> <li>• <a href="#">RADIUS Attributes Required for Proxy Mobile IP</a></li> <li>• <a href="#">Configuring Default Subscriber Parameters in Home Agent Context</a></li> </ul>
PDIF	<ul style="list-style-type: none"> <li>• <a href="#">How Proxy Mobile IP Works in a WiFi Network with Multiple Authentication</a></li> <li>• <a href="#">Configuring FA Services</a></li> <li>• <a href="#">Configuring Proxy MIP HA Failover</a></li> <li>• <a href="#">Configuring HA Services</a></li> <li>• <a href="#">Configuring Subscriber Profile RADIUS Attributes</a></li> <li>• <a href="#">RADIUS Attributes Required for Proxy Mobile IP</a></li> <li>• <a href="#">Configuring Default Subscriber Parameters in Home Agent Context</a></li> </ul>

## Proxy Mobile IP in 3GPP2 Service

For subscriber sessions using Proxy Mobile IP, R-P and PPP sessions get established between the MN and the PDSN as they would for a Simple IP session. However, the PDSN/FA performs Mobile IP operations with an HA (identified by information stored in the subscriber's profile) on behalf of the MN (i.e. the MN is only responsible for maintaining the Simple IP PPP session with PDSN).

The MN is assigned an IP address by either the PDSN/FA or the HA. Regardless of its source, the address is stored in a mobile binding record (MBR) stored on the HA. Therefore, as the MN roams through the service provider's network, each time a hand-off occurs, the MN will continue to use the same IP address stored in the MBR on the HA.

Note that unlike Mobile IP-capable MNs that can perform multiple sessions over a single PPP link, Proxy Mobile IP allows only a single session over the PPP link. In addition, simultaneous Mobile and Simple IP sessions will not be supported for an MN by the FA that is currently facilitating a Proxy Mobile IP session for the MN.

The MN is assigned an IP address by either the HA, a AAA server, or on a static-basis. The address is stored in a mobile binding record (MBR) stored on the HA. Therefore, as the MN roams through the service provider's network, each time a hand-off occurs, the MN will continue to use the same IP address stored in the MBR on the HA.

## Proxy Mobile IP in 3GPP Service

For IP PDP contexts using Proxy Mobile IP, the MN establishes a session with the GGSN as it normally would. However, the GGSN/FA performs Mobile IP operations with an HA (identified by information stored in the subscriber's profile) on behalf of the MN (i.e. the MN is only responsible for maintaining the IP PDP context with the GGSN, no Agent Advertisement messages are communicated with the MN).

The MN is assigned an IP address by either the HA, a AAA server, or on a static-basis. The address is stored in a mobile binding record (MBR) stored on the HA. Therefore, as the MN roams through the service provider's network, each time a hand-off occurs, the MN will continue to use the same IP address stored in the MBR on the HA.

Proxy Mobile IP can be performed on a per-subscriber basis based on information contained in their user profile, or for all subscribers facilitated by a specific APN. In the case of non-transparent IP PDP contexts, attributes returned from the subscriber's profile take precedence over the configuration of the APN.

## Proxy Mobile IP in WiMAX Service

For subscriber sessions using Proxy Mobile subscriber sessions get established between the MN and the ASN GW as they would for a Simple IP session. However, the ASN GW/FA performs Mobile IP operations with an HA (identified by information stored in the subscriber's profile) on behalf of the MN (i.e. the MN is only responsible for maintaining the Simple IP subscriber session with ASN GW).

The MN is assigned an IP address by either the ASN GW/FA or the HA. Regardless of its source, the address is stored in a mobile binding record (MBR) stored on the HA. Therefore, as the MN roams through the service provider's network, each time a hand-off occurs, the MN will continue to use the same IP address stored in the MBR on the HA.

Note that unlike Mobile IP-capable MNs that can perform multiple sessions over a single session link, Proxy Mobile IP allows only a single session over the session link. In addition, simultaneous Mobile and Simple IP sessions will not be supported for an MN by the FA that is currently facilitating a Proxy Mobile IP session for the MN.



## How Proxy Mobile IP Works in 3GPP2 Network

This section contains call flows displaying successful Proxy Mobile IP session setup scenarios. There are multiple scenarios that are dependant on how the MN receives an IP address. The following scenarios are described:

- **Scenario 1:** The AAA server that authenticates the MN at the PDSN allocates an IP address to the MN. Note that the PDSN does not allocate an address from its IP pools.
- **Scenario 2:** The HA assigns an IP address to the MN from one of its locally configured dynamic pools.

### Scenario 1: AAA server and PDSN/FA Allocate IP Address

The following figure and table display and describe a call flow in which the MN receives its IP address from the AAA server and PDSN/FA.

Figure 76. AAA/PDSN Assigned IP Address Proxy Mobile IP Call Flow

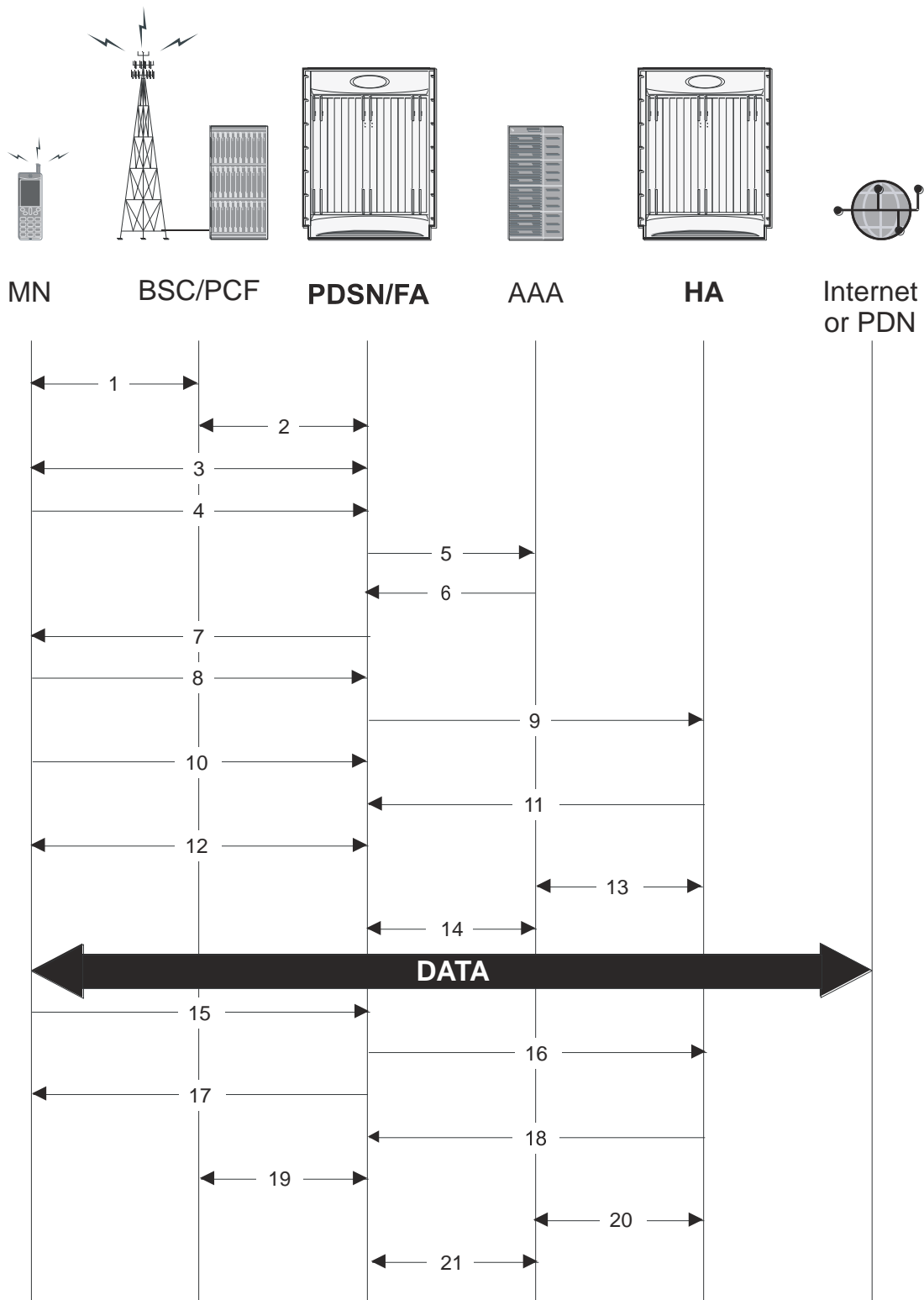


Table 37. AAA/PDSN Assigned IP Address Proxy Mobile IP Call Flow Description

Step	Description
1	Mobile Node (MN) secures a traffic channel over the airlink with the RAN through the BSC/PCF.
2	The PCF and PDSN/FA establish the R-P interface for the session.
3	The PDSN/FA and MN negotiate Link Control Protocol (LCP).
4	Upon successful LCP negotiation, the MN sends a PPP Authentication Request message to the PDSN/FA.
5	The PDSN/FA sends an Access Request message to the RADIUS AAA server.
6	The RADIUS AAA server successfully authenticates the subscriber and returns an Access Accept message to the PDSN/FA. The Accept message may contain various attributes to be assigned to the MN including the MN's Home Address (IP address) and the IP address of the HA to use.
7	The PDSN/FA sends a PPP Authentication Response message to the MN.
8	The MN sends an Internet Protocol Control Protocol (IPCP) Configuration Request message to the PDSN/FA with an MN address of 0.0.0.0.
9	The PDSN/FA forwards a Proxy Mobile IP Registration Request message to the HA. The message includes fields such as the MN's home address, the IP address of the FA (the care-of-address), and the FA-HA extension (security parameter index (SPI)).
10	While the FA is communicating with the HA, the MN may send additional IPCP Configuration Request messages.
11	The HA responds with a Proxy Mobile IP Registration Response after validating the home address against its pool. The HA also creates a mobile binding record (MBR) for the subscriber session.
12	The MN and the PDSN/FA negotiate IPCP. The result is that the MN is assigned the home address originally specified by the AAA server.
13	While the MN and PDSN/FA are negotiating IPCP, the HA and AAA server initiate accounting.
14	Upon completion of the IPCP negotiation, the PDSN/FA and AAA server initiate accounting fully establishing the session allowing the MN to send/receive data to/from the PDN.
15	Upon completion of the session, the MN sends an LCP Terminate Request message to the PDSN to end the PPP session.
16	The PDSN/FA sends a Proxy Mobile IP De-registration Request message to the HA.
17	The PDSN/FA send an LCP Terminate Acknowledge message to the MN ending the PPP session.
18	The HA sends a Proxy Mobile IP De-Registration Response message to the FA terminating the Pi interface
19	The PDSN/FA and the PCF terminate the R-P session.
20	The HA and the AAA server stop accounting for the session.
21	The PDSN and the AAA server stop accounting for the session.

## Scenario 2: HA Allocates IP Address

The following figure and table display and describe a call flow in which the MN receives its IP address from the HA.

Figure 77. HA Assigned IP Address Proxy Mobile IP Call Flow

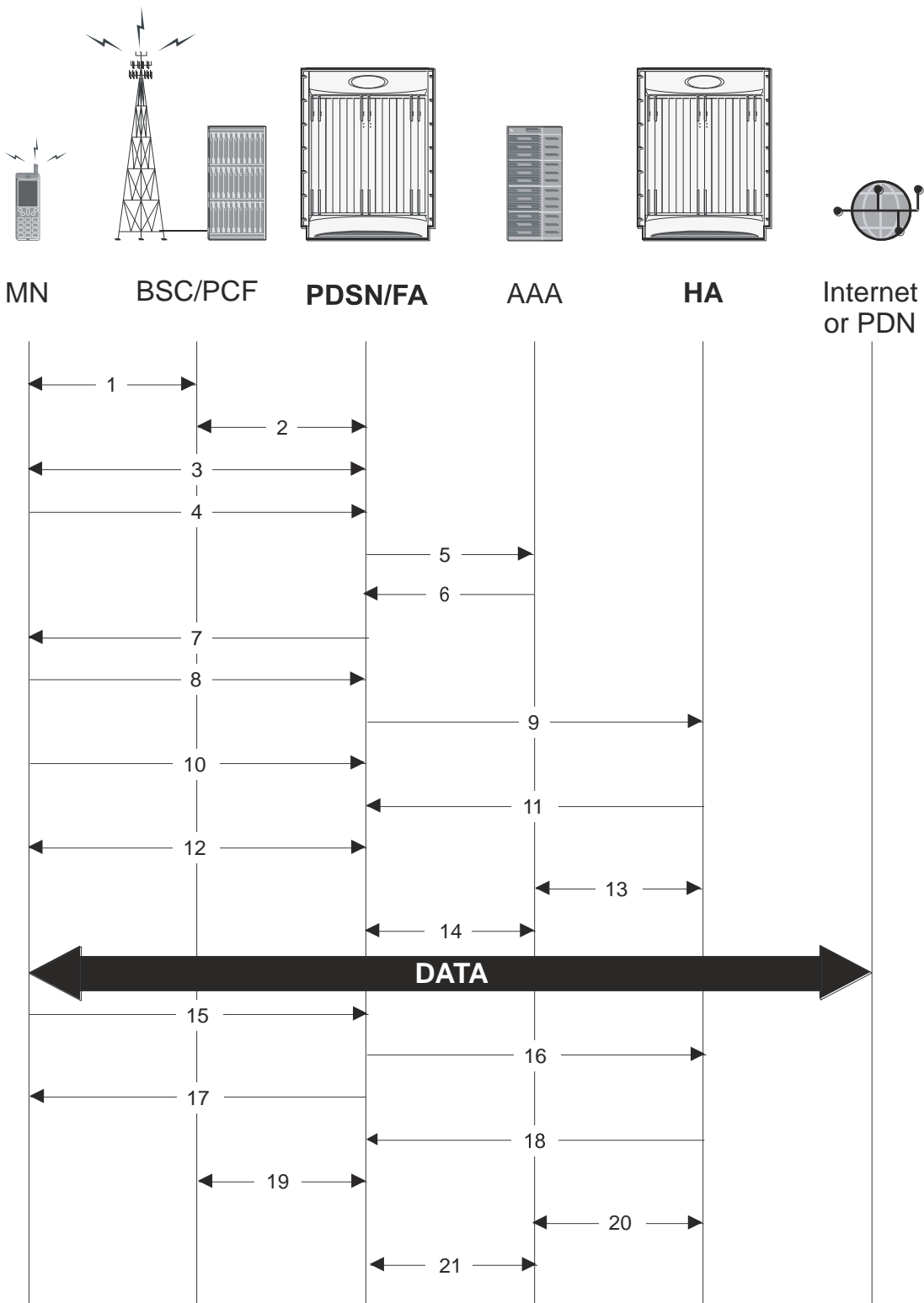


Table 38. HA Assigned IP Address Proxy Mobile IP Call Flow Description

Step	Description
1	Mobile Node (MN) secures a traffic channel over the airlink with the RAN through the BSC/PCF.
2	The PCF and PDSN/FA establish the R-P interface for the session.
3	The PDSN/FA and MN negotiate Link Control Protocol (LCP).
4	Upon successful LCP negotiation, the MN sends a PPP Authentication Request message to the PDSN/FA.
5	The PDSN/FA sends an Access Request message to the RADIUS AAA server.
6	The RADIUS AAA server successfully authenticates the subscriber and returns an Access Accept message to the PDSN/FA. The Accept message may contain various attributes to be assigned to the MN including the IP address of the HA to use.
7	The PDSN/FA sends a PPP Authentication Response message to the MN.
8	The MN sends an Internet Protocol Control Protocol (IPCP) Configuration Request message to the PDSN/FA with an MN address of 0.0.0.0.
9	The PDSN/FA forwards a Proxy Mobile IP Registration Request message to the HA. The message includes fields such as a Home Address indicator of 0.0.0.0, the IP address of the FA (the care-of-address), the IP address of the FA (the care-of-address), and the FA-HA extension (security parameter index (SPI)).
10	While the FA is communicating with the HA, the MN may send additional IPCP Configuration Request messages.
11	The HA responds with a Proxy Mobile IP Registration Response. The response includes an IP address from one of its locally configured pools to assign to the MN (its Home Address). The HA also creates a mobile binding record (MBR) for the subscriber session.
12	The MN and the PDSN/FA negotiate IPCP. The result is that the MN is assigned the home address originally specified by the AAA server.
13	While the MN and PDSN/FA are negotiating IPCP, the HA and AAA server initiate accounting.
14	Upon completion of the IPCP negotiation, the PDSN/FA and AAA server initiate accounting fully establishing the session allowing the MN to send/receive data to/from the PDN.
15	Upon completion of the session, the MN sends an LCP Terminate Request message to the PDSN to end the PPP session.
16	The PDSN/FA sends a Proxy Mobile IP De-registration Request message to the HA.
17	The PDSN/FA send an LCP Terminate Acknowledge message to the MN ending the PPP session.
18	The HA sends a Proxy Mobile IP De-Registration Response message to the FA terminating the Pi interface
19	The PDSN/FA and the PCF terminate the R-P session.
20	The HA and the AAA server stop accounting for the session.
21	The PDSN and the AAA server stop accounting for the session.

## How Proxy Mobile IP Works in 3GPP Network

This section contains call flows displaying successful Proxy Mobile IP session setup scenarios in 3GPP network.

The following figure and the text that follows describe a sample successful Proxy Mobile IP session setup call flow in 3GPP service.

Figure 78. Proxy Mobile IP Call Flow in 3GPP

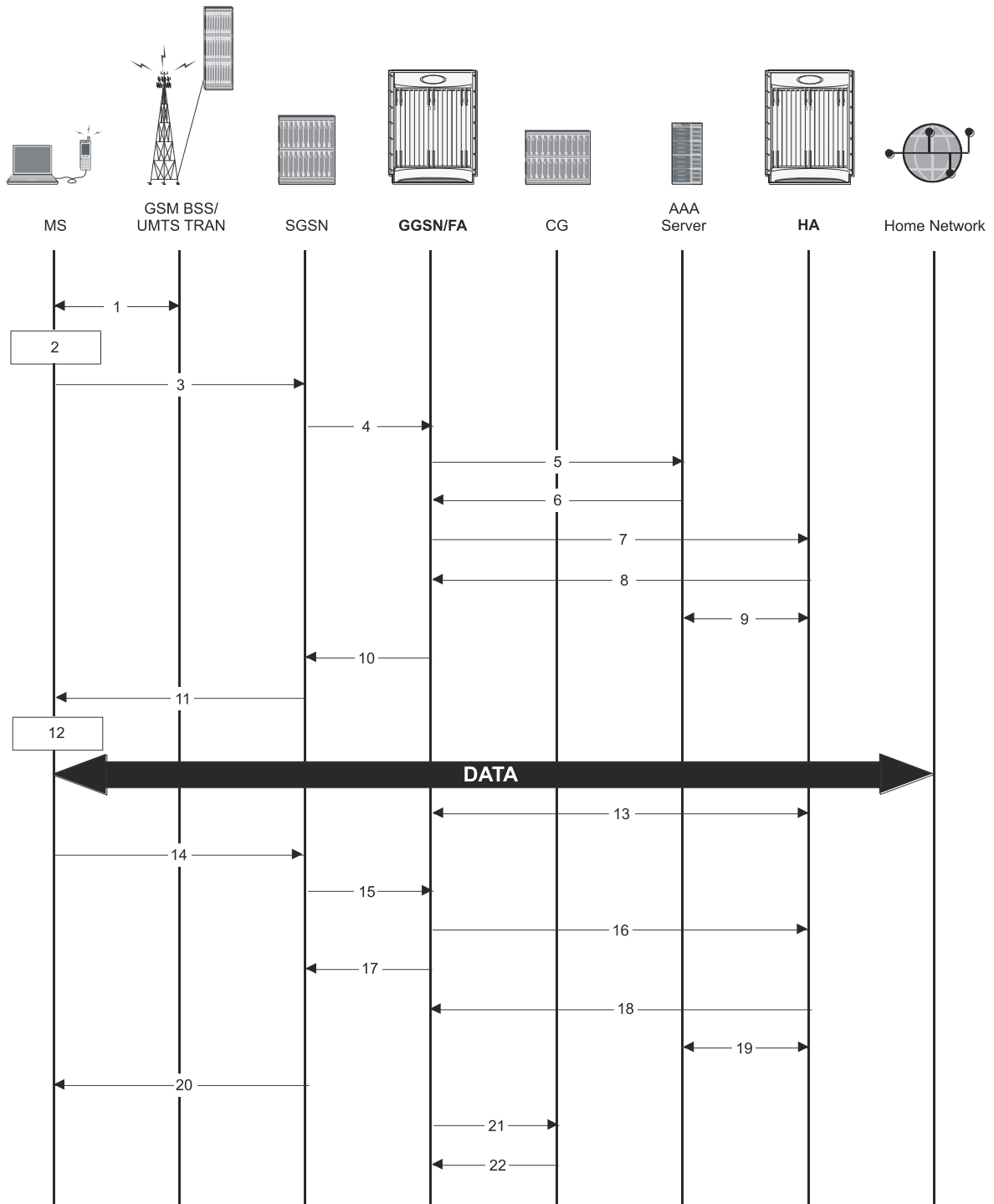


Table 39. Proxy Mobile IP Call Flow in 3GPP Description

Step	Description
------	-------------

Step	Description
1	The mobile station (MS) goes through the process of attaching itself to the GPRS/UMTS network.
2	<p>The terminal equipment (TE) aspect of the MS sends AT commands to the mobile terminal (MT) aspect of the MS to place it into PPP mode.</p> <p>The Link Control Protocol (LCP) is then used to configure the Maximum-Receive Unit size and the authentication protocol (Challenge-Handshake Authentication Protocol (CHAP), Password Authentication Protocol (PAP), or none). If CHAP or PAP is used, the TE will authenticate itself to the MT, which, in turn, stores the authentication information.</p> <p>Upon successful authentication, the TE sends an Internet Protocol Control Protocol (IPCP) Configure-Request message to the MT. The message will either contain a static IP address to use or request that one be dynamically assigned.</p>
3	The MS sends an Activate PDP Context Request message that is received by an SGSN. The message contains information about the subscriber such as the Network layer Service Access Point Identifier (NSAPI), PDP Type, PDP Address, Access Point Name (APN), quality of service (QoS) requested, and PDP configuration options.
4	The SGSN authenticates the request message and sends a Create PDP Context Request message to a GGSN using the GPRS Tunneling Protocol (GTPC, “C” indicates the control signaling aspect of the protocol). The recipient GGSN is selected based on either the request of the MS or is automatically selected by the SGSN. The message consists of various information elements including: PDP Type, PDP Address, APN, charging characteristics, and tunnel endpoint identifier (TEID, if the PDP Address was static).
5	<p>The GGSN determines if it can facilitate the session (in terms of memory or CPU resources, configuration, etc.) and creates a new entry in its PDP context list and provides a Charging ID for the session.</p> <p>From the APN specified in the message, the GGSN determines whether or not the subscriber is to be authenticated, if Proxy Mobile IP is to be supported for the subscriber, and if so, the IP address of the HA to contact.</p> <p>Note that Proxy Mobile IP support can also be determined by attributes in the user’s profile. Attributes in the user’s profile supersede APN settings.</p> <p>If authentication is required, the GGSN attempts to authenticate the subscriber locally against profiles stored in memory or send a RADIUS Access-Request message to a AAA server.</p>
6	If the GGSN authenticated the subscriber to a AAA server, the AAA server responds with a RADIUS Access-Accept message indicating successful authentication and any attributes for handling the subscriber PDP context.
7	If Proxy Mobile IP support was either enabled in the APN or in the subscriber’s profile, the GGSN/FA forwards a Proxy Mobile IP Registration Request message to the specified HA. The message includes such things as the MS’s home address, the IP address of the FA (the care-of-address), and the FA-HA extension (security parameter index (SPI)).
8	The HA responds with a Proxy Mobile IP Registration Response. The response includes an IP address from one of its locally configured pools to assign to the MS (its Home Address). The HA also creates a mobile binding record (MBR) for the subscriber session.
9	The HA sends an RADIUS Accounting Start request to the AAA server which the AAA server responds to.
10	The GGSN replies with an affirmative Create PDP Context Response using GTPC. The response will contain information elements such as the PDP Address representing either the static address requested by the MS or the address assigned by the GGSN, the TEID used to reference PDP Address, and PDP configuration options specified by the GGSN.
11	The SGSN returns an Activate PDP Context Accept message to the MS. The message includes response to the configuration parameters sent in the initial request.
12	<p>The MT, will respond to the TE’s IPCP Config-request with an IPCP Config-Ack message.</p> <p>The MS can now send and receive data to or from the PDN until the session is closed or times out. Note that for Mobile IP, only one PDP context is supported for the MS.</p>
13	The FA periodically sends Proxy Mobile IP Registration Request Renewal messages to the HA. The HA sends responses for each request.
14	The MS can terminate the data session at any time. To terminate the session, the MS sends a Deactivate PDP Context Request message that is received by the SGSN.



Step	Description
15	The SGSN sends a Delete PDP Context Request message to the GGSN facilitating the data session. The message includes the information elements necessary to identify the PDP context (i.e., TEID, and NSAPI).
16	The GGSN removes the PDP context from memory and the FA sends a Proxy Mobile IP Deregistration Request message to the HA.
17	The GGSN returns a Delete PDP Context Response message to the SGSN.
18	The HA replies to the FA with a Proxy Mobile IP Deregistration Request Response.
19	The HA sends an RADIUS Accounting Stop request to the AAA server which the AAA server responds to.
20	The SGSN returns a Deactivate PDP Context Accept message to the MS.
21	The GGSN delivers the GGSN Charging Detail Records (G-CDRs) to a charging gateway (CG) using GTP Prime (GTPP). Note that, though not shown in this example, the GGSN could optionally be configured to send partial CDRs while the PDP context is active.
22	For each accounting message received from the GGSN, the CG responds with an acknowledgement.

# How Proxy Mobile IP Works in WiMAX Network

This section contains call flows displaying successful Proxy Mobile IP session setup scenarios. There are multiple scenarios that are dependant on how the MN receives an IP address. The following scenarios are described:

- **Scenario 1:** The AAA server that authenticates the MN at the ASN GW allocates an IP address to the MN. Note that the ASN GW does not allocate an address from its IP pools.
- **Scenario 2:** The HA assigns an IP address to the MN from one of its locally configured dynamic pools.

## Scenario 1: AAA server and ASN GW/FA Allocate IP Address

The following figure and table display and describe a call flow in which the MN receives its IP address from the AAA server and ASN GW/FA.

Figure 79. AAA/ASN GW Assigned IP Address Proxy Mobile IP Call Flow

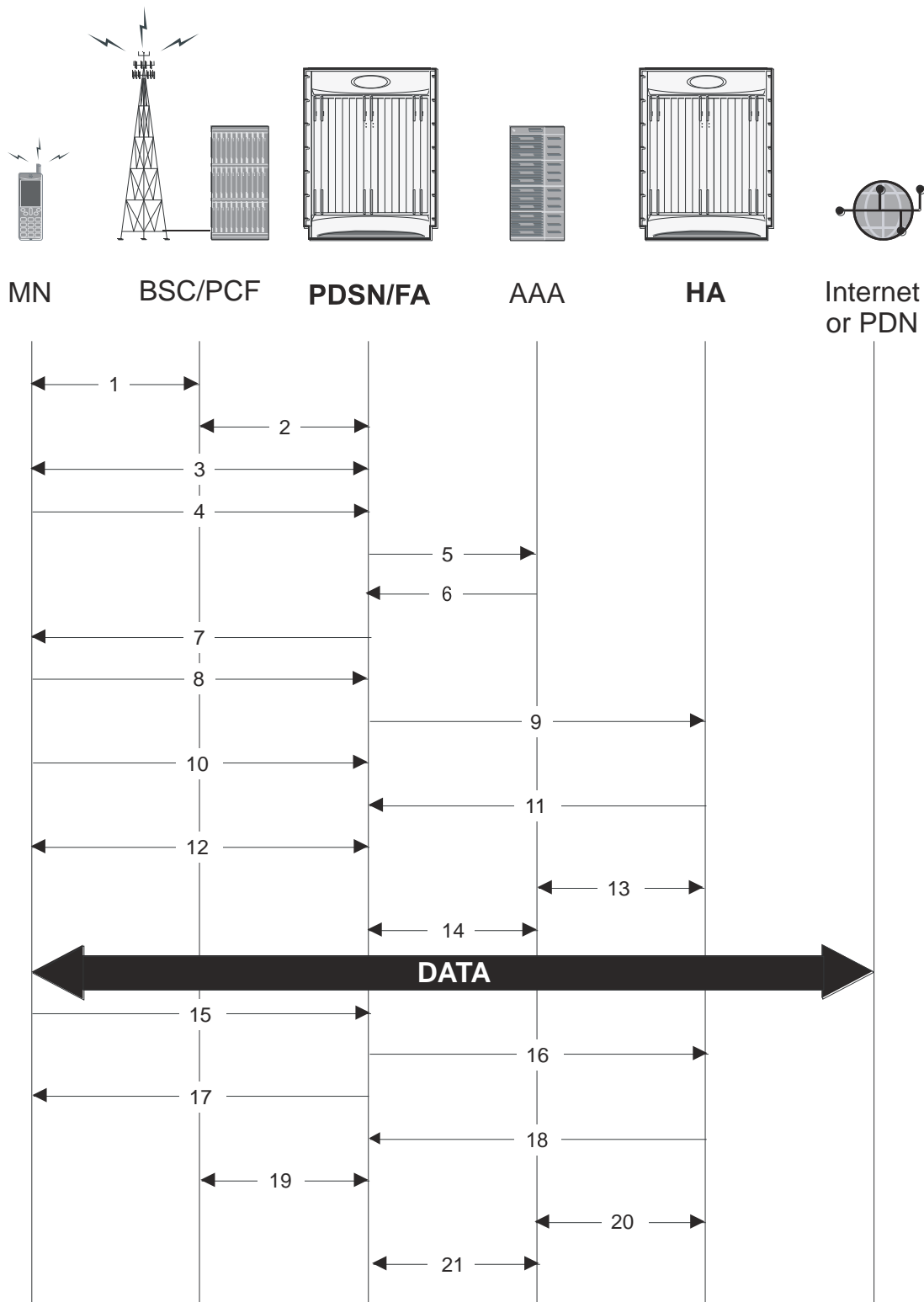


Table 40. AAA/ASN GW Assigned IP Address Proxy Mobile IP Call Flow Description

Step	Description
1	Mobile Node (MN) secures a traffic channel over the airlink with the BS.
2	The BS and ASN GW/FA establish the R6 interface for the session.
3	The ASN GW/FA and MN negotiate Link Control Protocol (LCP).
4	Upon successful LCP negotiation, the MN sends a PPP Authentication Request message to the ASN GW/FA.
5	The ASN GW/FA sends an Access Request message to the RADIUS AAA server.
6	The RADIUS AAA server successfully authenticates the subscriber and returns an Access Accept message to the ASN GW/FA. The Accept message may contain various attributes to be assigned to the MN including the MN's Home Address (IP address) and the IP address of the HA to use.
7	The ASN GW/FA sends a EAP Authentication Response message to the MN.
8	The MN sends an Internet Protocol Control Protocol (IPCP) Configuration Request message to the ASN GW/FA with an MN address of 0.0.0.0.
9	The ASN GW/FA forwards a Proxy Mobile IP Registration Request message to the HA. The message includes fields such as the MN's home address, the IP address of the FA (the care-of-address), and the FA-HA extension (security parameter index (SPI)).
10	While the FA is communicating with the HA, the MN may send additional IPCP Configuration Request messages.
11	The HA responds with a Proxy Mobile IP Registration Response after validating the home address against its pool. The HA also creates a mobile binding record (MBR) for the subscriber session.
12	The MN and the ASN GW/FA negotiate IPCP. The result is that the MN is assigned the home address originally specified by the AAA server.
13	While the MN and ASN GW/FA are negotiating IPCP, the HA and AAA server initiate accounting.
14	Upon completion of the IPCP negotiation, the ASN GW/FA and AAA server initiate accounting fully establishing the session allowing the MN to send/receive data to/from the PDN.
15	Upon completion of the session, the MN sends an LCP Terminate Request message to the ASN GW to end the subscriber session.
16	The PDSN/FA sends a Proxy Mobile IP De-registration Request message to the HA.
17	The ASN GW/FA send an LCP Terminate Acknowledge message to the MN ending the subscriber session.
18	The HA sends a Proxy Mobile IP De-Registration Response message to the FA terminating the R3 interface
19	The ASN GW/FA and the BS terminate the R6 session.
20	The HA and the AAA server stop accounting for the session.
21	The ASN GW and the AAA server stop accounting for the session.

## Scenario 2: HA Allocates IP Address

The following figure and table display and describe a call flow in which the MN receives its IP address from the HA.

Figure 80. HA Assigned IP Address Proxy Mobile IP Call Flow

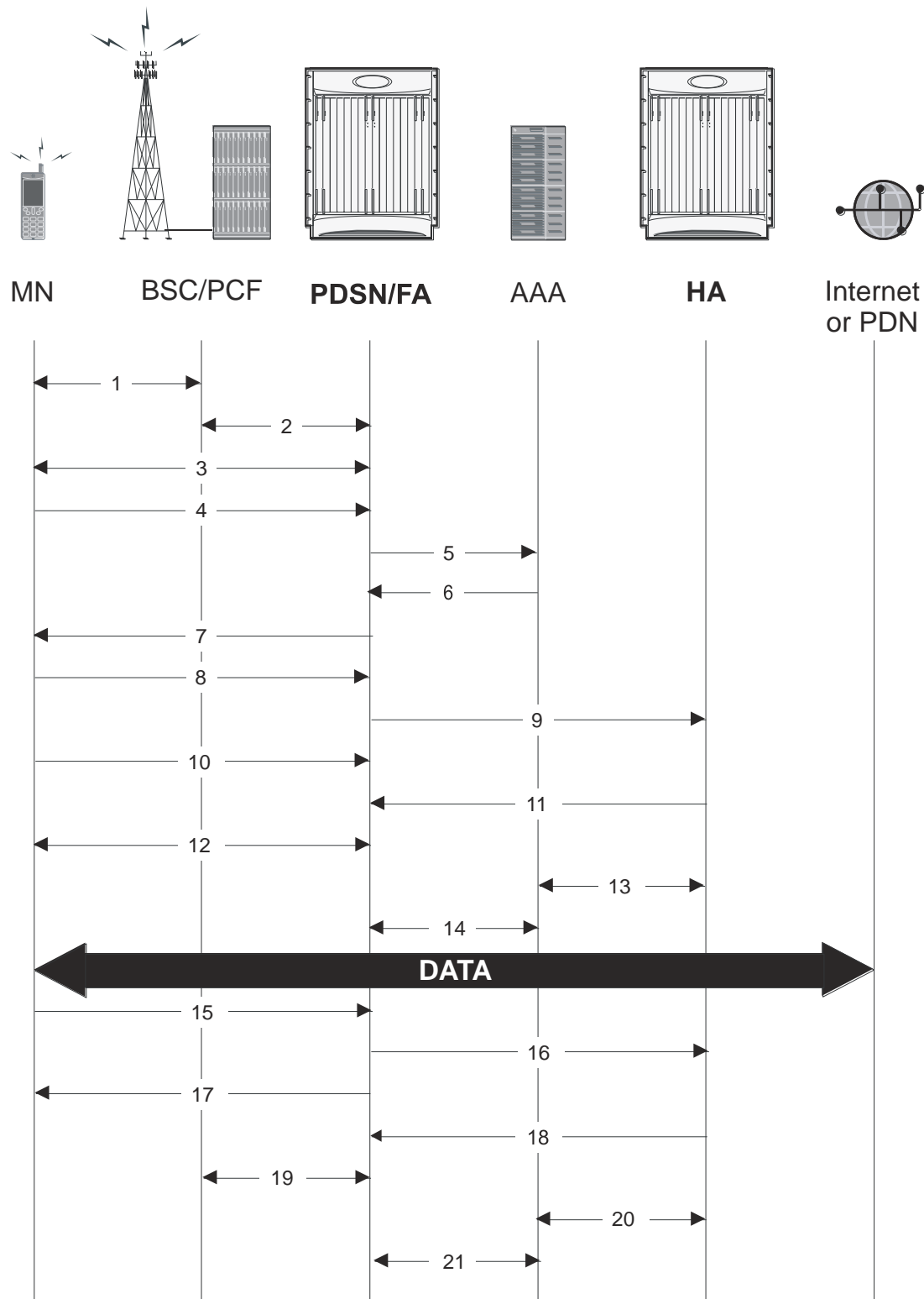


Table 41. HA Assigned IP Address Proxy Mobile IP Call Flow Description

Step	Description
1	Mobile Node (MN) secures a traffic channel over the airlink with the BS.
2	The BS and ASN GW/FA establish the R6 interface for the session.
3	The ASN GW/FA and MN negotiate Link Control Protocol (LCP).
4	Upon successful LCP negotiation, the MN sends an EAP Authentication Request message to the ASN GW/FA.
5	The ASN GW/FA sends an Access Request message to the RADIUS AAA server.
6	The RADIUS AAA server successfully authenticates the subscriber and returns an Access Accept message to the ASN GW/FA. The Accept message may contain various attributes to be assigned to the MN including the IP address of the HA to use.
7	The ASN GW/FA sends an EAP Authentication Response message to the MN.
8	The MN sends an Internet Protocol Control Protocol (IPCP) Configuration Request message to the ASN GW/FA with an MN address of 0.0.0.0.
9	The ASN GW/FA forwards a Proxy Mobile IP Registration Request message to the HA. The message includes fields such as a Home Address indicator of 0.0.0.0, the IP address of the FA (the care-of-address), the IP address of the FA (the care-of-address), and the FA-HA extension (security parameter index (SPI)).
10	While the FA is communicating with the HA, the MN may send additional IPCP Configuration Request messages.
11	The HA responds with a Proxy Mobile IP Registration Response. The response includes an IP address from one of its locally configured pools to assign to the MN (its Home Address). The HA also creates a mobile binding record (MBR) for the subscriber session.
12	The MN and the ASN GW/FA negotiate IPCP. The result is that the MN is assigned the home address originally specified by the AAA server.
13	While the MN and ASN GW/FA are negotiating IPCP, the HA and AAA server initiate accounting.
14	Upon completion of the IPCP negotiation, the ASN GW/FA and AAA server initiate accounting fully establishing the session allowing the MN to send/receive data to/from the PDN.
15	Upon completion of the session, the MN sends an LCP Terminate Request message to the ASN GW to end the subscriber session.
16	The ASN GW/FA sends a Proxy Mobile IP De-registration Request message to the HA.
17	The ASN GW/FA send an LCP Terminate Acknowledge message to the MN ending the PPP session.
18	The HA sends a Proxy Mobile IP De-Registration Response message to the FA terminating the R3 interface
19	The ASN GW/FA and the BS terminate the R6 session.
20	The HA and the AAA server stop accounting for the session.
21	The ASN GW and the AAA server stop accounting for the session.

## How Proxy Mobile IP Works in a WiFi Network with Multiple Authentication

Proxy-Mobile IP was developed as a result of networks of Mobile Subscribers (MS) that are not capable of Mobile IP operation. In this scenario a PDIF acts a mobile IP client and thus implements Proxy-MIP support.

Although not required or necessary in a Proxy-MIP network, this implementation uses a technique called Multiple Authentication. In Multi-Auth arrangements, the device is authenticated first using HSS servers. Once the device is authenticated, then the subscriber is authenticated over a RADIUS interface to AAA servers. This supports existing EV-DO servers in the network.

The MS first tries to establish an IKEv2 session with the PDIF. The MS uses the EAP-AKA authentication method for the initial device authentication using Diameter over SCTP over IPv6 to communicate with HSS servers. After the initial Diameter EAP authentication, the MS continues with EAP MD5/GTC authentication.

After successful device authentication, PDIF then uses RADIUS to communicate with AAA servers for the subscriber authentication. It is assumed that RADIUS AAA servers do not use EAP methods and hence RADIUS messages do not contain any EAP attributes.

Assuming a successful RADIUS authentication, PDIF then sets up the IPSec Child SA tunnel using a Tunnel Inner Address (TIA) for passing control traffic only. PDIF receives the MS address from the Home Agent, and passes it on to the MS through the final AUTH response in the IKEv2 exchange.

When IPSec negotiation finishes, the PDIF assigns a home address to the MS and establishes a CHILD SA to pass data. The initial TIA tunnel is torn down and the IP address returned to the address pool. The PDIF then generates a RADIUS accounting START message.

When the session is disconnected, the PDIF generates a RADIUS accounting STOP message.

The following figures describe a Proxy-MIP session setup using CHAP authentication (EAP-MD5), but also addresses a PAP authentication setup using EAP-GTC when EAP-MD5 is not supported by either PDIF or MS.

Figure 81. Proxy-MIP Call Setup using CHAP Authentication

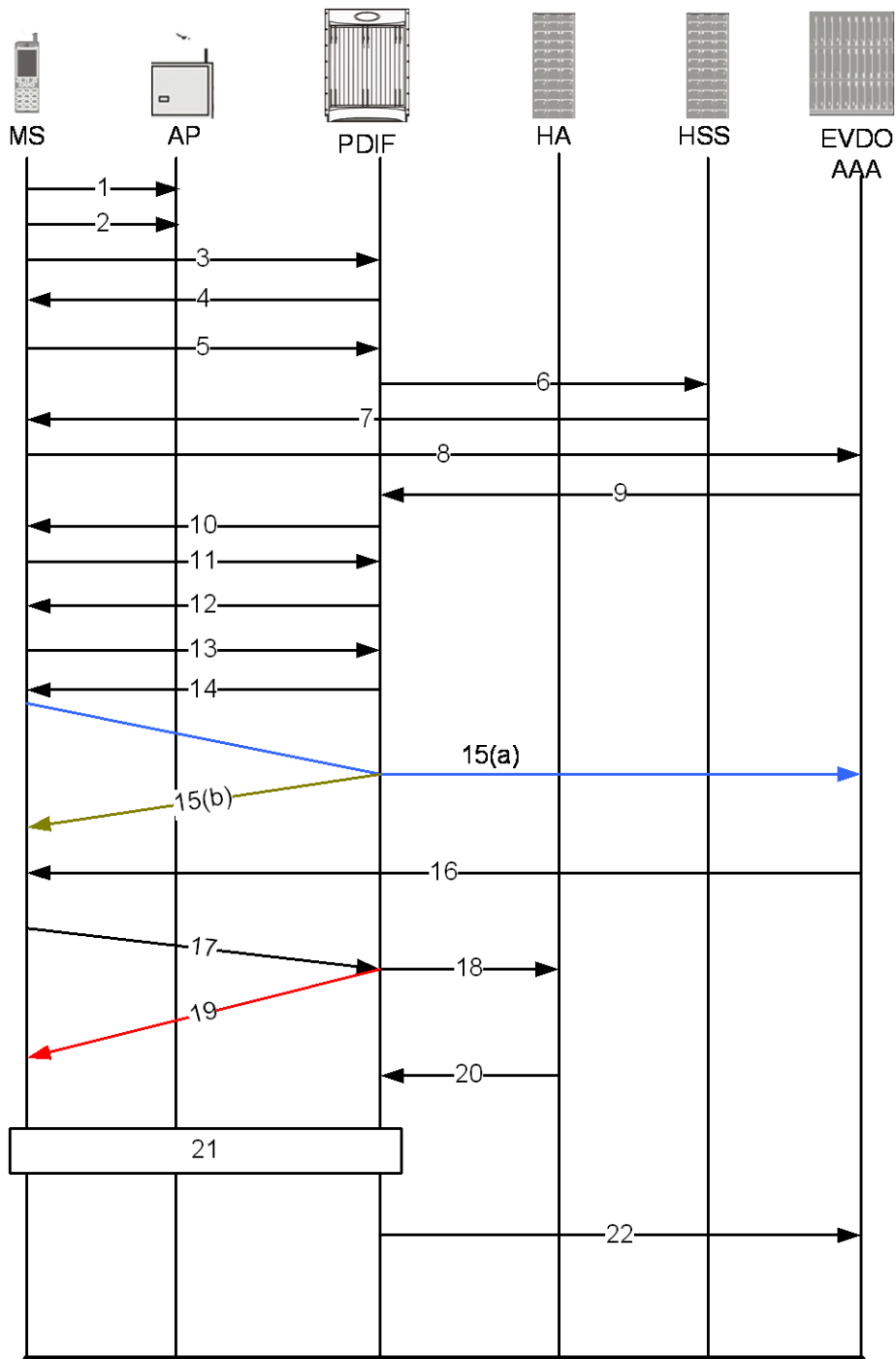


Table 42. Proxy-MIP Call Setup using CHAP Authentication

Step	Description
------	-------------



Step	Description
1	On connecting to WiFi network, MS first send DNS query to get PDIF IP address
2	MS receives PDIF address from DNS
3	MS sets up IKEv2/IPSec tunnel by sending IKE_SA_INIT Request to PDIF. MS includes SA, KE, Ni, NAT-DETECTION Notify payloads in the IKEv2 exchange.
4	PDIF processes the IKE_SA_INIT Request for the appropriate PDIF service (bound by the destination IP address in the IKEv2 INIT request). PDIF responds with IKE_SA_INIT Response with SA, KE, Nr payloads and NAT-Detection Notify payloads. If multiple-authentication support is configured to be enabled in the PDIF service, PDIF will include MULTIPLE_AUTH_SUPPORTED Notify payload in the IKE_SA_INIT Response. PDIF will start the IKEv2 setup timer after sending the IKE_SA_INIT Response.
5	On receiving successful IKE_SA_INIT Response from PDIF, MS sends IKE_AUTH Request for the first EAP-AKA authentication. If the MS is capable of doing multiple-authentication, it will include MULTI_AUTH_SUPPORTED Notify payload in the IKE_AUTH Request. MS also includes IDi payload which contains the NAI, SA, TSr, CP (requesting IP address and DNS address) payloads. MS will not include AUTH payload to indicate that it will use EAP methods.
6	On receiving IKE_AUTH Request from MS, PDIF sends DER message to Diameter AAA server. AAA servers are selected based on domain profile, default subscriber template or default domain configurations. PDIF includes Multiple-Auth-Support AVP, EAP-Payload AVP with EAP-Response/Identity in the DER. Exact details are explained in the Diameter message sections. PDIF starts the session setup timer on receiving IKE_AUTH Request from MS.
7	PDIF receives DEA with Result-Code AVP specifying to continue EAP authentication. PDIF takes EAP-Payload AVP contents and sends IKE_AUTH Response back to MS in the EAP payload. PDIF allows IDr and CERT configurations in the PDIF service and optionally includes IDr and CERT payloads (depending upon the configuration). PDIF optionally includes AUTH payload in IKE_AUTH Response if PDIF service is configured to do so.
8	MS receives the IKE_AUTH Response from PDIF. MS processes the exchange and sends a new IKE_AUTH Request with EAP payload. PDIF receives the new IKE_AUTH Request from MS and sends DER to AAA server. This DER message contains the EAP-Payload AVP with EAP-AKA challenge response and challenge received from MS.
9	The AAA server sends the DEA back to the PDIF with Result-Code AVP as “success.” The EAP-Payload AVP message also contains the EAP result code with “success.” The DEA also contains the IMSI for the user, which is included in the Callback-Id AVP. PDIF uses this IMSI for all subsequent session management functions such as duplicate session detection etc. PDIF also receives the MSK from AAA, which is used for further key computation.
10	PDIF sends the IKE_AUTH Response back to MS with the EAP payload.
11	MS sends the final IKE_AUTH Request for the first authentication with the AUTH payload computed from the keys. If the MS plans to do the second authentication, it will include ANOTHER_AUTH_FOLLOWS Notify payload also.
12	PDIF processes the AUTH request and responds with the IKE_AUTH Response with the AUTH payload computed from the MSK. PDIF does not assign any IP address for the MS pending second authentication. Nor will the PDIF include any configuration payloads. a. If PDIF service does not support Multiple-Authentication and ANOTHER_AUTH_FOLLOWS Notify payload is received, then PDIF sends IKE_AUTH Response with appropriate error and terminate the IKEv2 session by sending INFORMATIONAL (Delete) Request.b. If ANOTHER_AUTH_FOLLOWS Notify payload is not present in the IKE_AUTH Request, PDIF allocates the IP address from the locally configured pools. However, if <b>proxy-mip-required</b> is enabled, then PDIF initiates Proxy-MIP setup to HA by sending P-MIP RRQ. When PDIF receives the Proxy-MIP RRP, it takes the Home Address (and DNS addresses if any) and sends the IKE_AUTH Response back to MS by including CP payload with Home Address and DNS addresses. In either case, IKEv2 setup will finish at this stage and IPSec tunnel gets established with a Tunnel Inner Address (TIA).
13	MS does the second authentication by sending the IKE_AUTH Request with IDi payload to include the NAI. This NAI may be completely different from the NAI used in the first authentication.

Step	Description
14	<p>On receiving the second authentication IKE_AUTH Request, PDIF checks the configured second authentication methods. The second authentication may be either EAP-MD5 (default) or EAP-GTC. The EAP methods may be either EAP-Passthru or EAP-Terminated.</p> <p>a. If the configured method is EAP-MD5, PDIF sends the IKE_AUTH Response with EAP payload including challenge.</p> <p>b. If the configured method is EAP-GTC, PDIF sends the IKE_AUTH Response with EAP-GTC.</p> <p>c. MS processes the IKE_AUTH Response:</p> <ul style="list-style-type: none"> <li>• If the MS supports EAP-MD5, and the received method is EAP-MD5, then the MS will take the challenge, compute the response and send IKE_AUTH Request with EAP payload including Challenge and Response.</li> <li>• If the MS does not support EAP-MD5, but EAP-GTC, and the received method is EAP-MD5, the MS sends legacy-Nak with EAP-GTC.</li> </ul>
15(a)	<p>PDIF receives the new IKE_AUTH Request from MS.</p> <p>If the original method was EAP-MD5 and MD5 challenge and response is received, PDIF sends RADIUS Access Request with corresponding attributes (Challenge, Challenge Response, NAI, IMSI etc.).</p>
15(b)	<p>If the original method was EAP-MD5 and legacy-Nak was received with GTC, the PDIF sends IKE_AUTH Response with EAP-GTC.</p>
16	PDIF receives Access Accept from RADIUS and sends IKE_AUTH Response with EAP success.
17	PDIF receives the final IKE_AUTH Request with AUTH payload.
18	PDIF checks the validity of the AUTH payload and initiates Proxy-MIP setup request to the Home Agent if <b>proxy-mip-required</b> is enabled. The HA address may be received from the RADIUS server in the Access Accept (Step 16) or may be locally configured. PDIF may also remember the HA address from the first authentication received in the final DEA message.
19	If <b>proxy-mip-required</b> is disabled, PDIF assigns the IP address from the local pool.
20	PDIF received proxy-MIP RRP and gets the IP address and DNS addresses.
21	PDIF sets up the IPSec tunnel with the home address. On receiving the IKE_AUTH Response MS also sets up the IPSec tunnel using the received IP address. PDIF sends the IKE_AUTH Response back to MS by including the CP payload with the IP address and optionally the DNS addresses. This completes the setup.
22	PDIF sends a RADIUS Accounting start message.



**Important:** For Proxy-MIP call setup using PAP, the first 14 steps are the same as for CHAP authentication. However, here they deviate because the MS does not support EAP-MD5 authentication, but EAP-GTC. In response to the EAP-MD5 challenge, the MS instead responds with legacy-Nak with EAP-GTC. The diagram below picks up at this point.

Figure 82. Proxy-MIP Call Setup using PAP Authentication

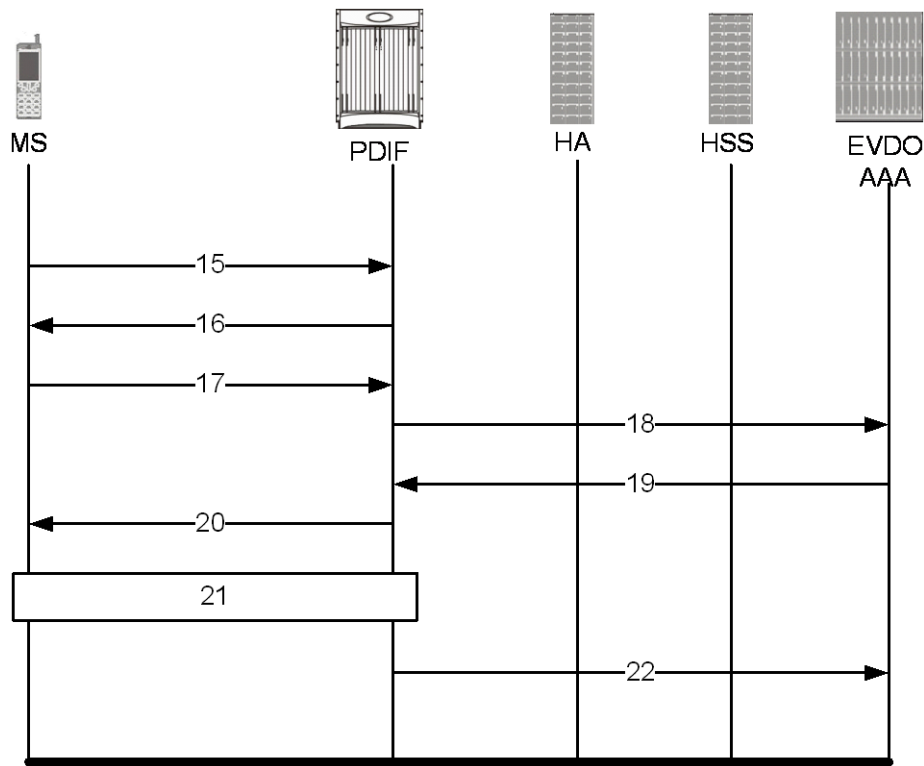


Table 43. Proxy-MIP Call Setup using PAP Authentication

Step	Description
15	MS is not capable of CHAP authentication but PAP authentication, and the MS returns the EAP payload to indicate that it needs EAP-GTC authentication.
16	PDIF then initiates EAP-GTC procedure, and requests a password from MS.
17	MS includes an authentication password in the EAP payload to PDIF.
18	Upon receipt of the password, PDIF sends a RADIUS Access Request which includes NAI in the User-Name attribute and PAP-password.
19	Upon successful authentication, the AAA server returns a RADIUS Access Accept message, which may include Framed-IP-Address attribute.
20	The attribute content in the Access Accept message is encoded as EAP payload with EAP success when PDIF sends the IKE_AUTH Response to the MS.
21	The MS and PDIF now have a secure IPsec tunnel for communication.
22	Pdif sends an Accounting START message.

# Configuring Proxy Mobile-IP Support

Support for Proxy Mobile-IP requires that the following configurations be made:



**Important:** Not all commands and keywords/variables may be supported. This depends on the platform type and the installed license(s).

- **FA service(s):** Proxy Mobile IP must be enabled, operation parameters must be configured, and FA-HA security associations must be specified.
- **HA service(s):** FA-HA security associations must be specified.
- **Subscriber profile(s):** Attributes must be configured to allow the subscriber(s) to use Proxy Mobile IP. These attributes can be configured in subscriber profiles stored locally on the system or remotely on a RADIUS AAA server.
- **APN template(s):** Proxy Mobile IP can be supported for every subscriber IP PDP context facilitated by a specific APN template based on the configuration of the APN.



**Important:** These instructions assume that the system was previously configured to support subscriber data sessions as a core network service and/or an HA according to the instructions described in the respective product administration guide.

## Configuring FA Services

Use this example to configure an FA service to support Proxy Mobile IP:

**configure**

**context** <context\_name>

**fa-service** <fa\_service\_name>

**proxy-mip** allow

**proxy-mip max-retransmissions** <integer>

**proxy-mip retransmission-timeout** <seconds>

**proxy-mip renew-percent-time** percentage

**fa-ha-spi remote-address** { ha\_ip\_address | ip\_addr\_mask\_combo } **spi-number** number { **encrypted secret** enc\_secret | **secret** secret } [ **description** string ] [ **hash-algorithm** { hmac-md5 | md5 | rfc2002-md5 } | **replay-protection** { timestamp | nonce } | **timestamp-tolerance** tolerance ]

**authentication mn-ha** allow-noauth

**end**

## Notes:

- The **proxy-mip max-retransmissions** command configures the maximum number re-try attempts that the FA service is allowed to make when sending Proxy Mobile IP Registration Requests to the HA.
- **proxy-mip retransmission-timeout** configures the maximum amount of time allowed by the FA for a response from the HA before re-sending a Proxy Mobile IP Registration Request message.
- **proxy-mip renew-percent-time** configures the amount of time that must pass prior to the FA sending a Proxy Mobile IP Registration Renewal Request.

## Example

If the advertisement registration lifetime configured for the FA service is 900 seconds and the renew-time is configured to 50%, then the FA requests a lifetime of 900 seconds in the Proxy MIP registration request. If the HA grants a lifetime of **600** seconds, then the FA sends the Proxy Mobile IP Registration Renewal Request message after **300** seconds have passed.

- Use the **fa-ha-spi remote-address** command to modify configured FA-HA SPIs to support Proxy Mobile IP. Refer to the *Command Line Interface Reference* for the full command syntax.



**Important:** Note that FA-HA SPIs **must** be configured for the Proxy-MIP feature to work, while it is optional for regular MIP.

- Use the **authentication mn-ha allow-noauth** command to configure the FA service to allow communications from the HA without authenticating the HA.

## Verify the FA Service Configuration

Use the following command to verify the configuration of the FA service:

```
show fa-service name <fa_service_name>
```

## Notes:

- Repeat this example as needed to configure additional FA services to support Proxy-MIP.
- Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Proceed to the optional [Configuring Proxy MIP HA Failover](#) section to configure Proxy MIP HA Failover support or skip to the [Configuring HA Services](#) section to configure HA service support for Proxy Mobile IP.

## Configuring Proxy MIP HA Failover

Use this example to configure Proxy Mobile IP HA Failover:



**Important:** This configuration in this section is optional.

When configured, Proxy MIP HA Failover provides a mechanism to use a specified alternate Home Agent for the subscriber session when the primary HA is not available. Use the following configuration example to configure the Proxy MIP HA Failover:

```

configure

context <context_name>

    fa-service <fa_service_name>

        proxy-mip ha-failover [ max-attempts <max_attempts> | num-attempts-
before-switching <num_attempts> | timeout <seconds> ]

```

Notes:

- Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

## Configuring HA Services

Use the following configuration example to configure HA services to support Proxy Mobile IP.

```

configure

context <context_name>

    ha-service <ha_service_name>

```



**Important:** Note that FA-HA SPIs must be configured for the Proxy MIP feature to work while it is optional for regular MIP. Also note that the above syntax assumes that FA-HA SPIs were previously configured as part of the HA service as described in respective product Administration Guide. The **replay-protection** and **timestamp-tolerance** keywords should only be configured when supporting Proxy Mobile IP.

```

    fa-ha-spi remote-address <fa_ip_address> spi-number <number> { encrypted secret
<enc_secret> | secret <secret> } [ description <string> ] [ hash-algorithm { hmac-md5 |
md5 | rfc2002-md5 } ] replay-protection { timestamp | nonce } | timestamp-tolerance
<tolerance> ]

    authentication mn-ha allow-noauth

    authentication mn-aaa allow-noauth

end

```

Notes:

- Repeat this example as needed to configure additional HA services to support Proxy-MIP.
- Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

To verify the configuration of the HA service:

```

context <context_name>


    show ha-service name <ha_service_name>

```

## Configuring Subscriber Profile RADIUS Attributes

In order for subscribers to use Proxy Mobile IP, attributes must be configured in their user profile or in an APN for 3GPP service. As mentioned previously, the subscriber profiles can be located either locally on the system or remotely on a RADIUS AAA server.


This section provides information on the RADIUS attributes that must be used and instructions for configuring locally stored profiles/APNs in support of Proxy Mobile IP.

 **Important:** Instructions for configuring RADIUS-based subscriber profiles are not provided in this document. Please refer to the documentation supplied with your server for further information.

### RADIUS Attributes Required for Proxy Mobile IP

The following table describes the attributes that must be configured in profiles stored on RADIUS AAA servers in order for the subscriber to use Proxy Mobile IP.

**Table 44.** Required RADIUS Attributes for Proxy Mobile IP

Attribute	Description	Values
SN-Subscriber-Permission OR SN1-Subscriber-Permission	Indicates the services allowed to be delivered to the subscriber. For Proxy Mobile IP, this attribute <b>must</b> be set to Simple IP.	<ul style="list-style-type: none"> <li>None (0)</li> <li>Simple IP (0x01)</li> <li>Mobile IP (0x02)</li> <li>Home Agent Terminated Mobile IP (0x04)</li> </ul>
SN-Proxy-MIP OR SN1-Proxy-MIP	Specifies if the configured service will perform compulsory Proxy-MIP tunneling for a Simple-IP subscriber. This attribute <b>must</b> be enabled to support Proxy Mobile IP.	<ul style="list-style-type: none"> <li>Disabled - do not perform compulsory Proxy-MIP (0)</li> <li>Enabled - perform compulsory Proxy-MIP (1)</li> </ul>
SN-Simultaneous-SIP-MIP OR SN1-Simultaneous-SIP-MIP	Indicates whether or not a subscriber can simultaneously access both Simple IP and Mobile IP services.   <b>Important:</b> Regardless of the configuration of this attribute, the FA facilitating the Proxy Mobile IP session will <b>not</b> allow simultaneous Simple IP and Mobile IP sessions for the MN.	<ul style="list-style-type: none"> <li>Disabled (0)</li> <li>Enabled (1)</li> </ul>

Attribute	Description	Values
SN-PDSN-Handoff-Req-IP-Addr OR SN1-PDSN-Handoff-Req-IP-Addr	Specifies whether or not the system should reject and terminate the subscriber session when the proposed address in IPCP by the mobile does not match the existing address that was granted by the chassis during an Inter-chassis handoff. This can be used to disable the acceptance of 0.0.0.0 as the IP address proposed by the MN during the IPCP negotiation that occurs during an Inter-chassis handoff. This attribute is disabled (do not reject) by default.	<ul style="list-style-type: none"> <li>Disabled - do not reject (0)</li> <li>Enabled - reject (1)</li> </ul>
3GPP2-MIP-HA-Address	This attribute sent in an Access-Accept message specifies the IP Address of the HA. Multiple attributes can be sent in Access Accept. However, only the first two are considered for processing. The first one is the primary HA and the second one is the secondary (alternate) HA used for HA Failover.	IPv4 Address

## Configuring Local Subscriber Profiles for Proxy-MIP on a PDSN

This section provides information and instructions for configuring local subscriber profiles on the system to support Proxy Mobile IP on a PDSN.

**configure**

```

context <context_name>

    subscriber name <subscriber_name>

    permission pdsn-simple-ip

    proxy-mip allow

    inter-pdsn-handoff require ip-address

    mobile-ip home-agent <ha_address>

    <optional> mobile-ip home-agent <ha_address> alternate

    ip context-name <context_name>

end

```

Verify that your settings for the subscriber(s) just configured are correct.

```
show subscribers configuration username <subscriber_name>
```

Notes:

- Configure the system to enforce the MN's use of its assigned IP address during IPCP negotiations resulting from inter-PDSN handoffs. Sessions re-negotiating IPCP will be rejected if they contain an address other than that which was granted by the PDSN (i.e. 0.0.0.0). This rule can be enabled by entering the **inter-pdsn-handoff require ip-address** command.
- Optional: If you have enabled the Proxy-MIP HA Failover feature, use the **mobile-ip home-agent ha\_address alternate** command to specify the secondary, or alternate HA.



- Repeat this example as needed to configure additional FA services to support Proxy-MIP.
- Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

## Configuring Local Subscriber Profiles for Proxy-MIP on a PDIF

This section provides instructions for configuring local subscriber profiles on the system to support Proxy Mobile IP on a PDIF.

**configure**

```
context <context-name>

    subscriber name <subscriber_name>

    proxy-mip require
```

Note

*subscriber\_name* is the name of the subscriber and can be from 1 to 127 alpha and/or numeric characters and is case sensitive.

## Configuring Default Subscriber Parameters in Home Agent Context

It is very important that the subscriber default, configured in the same context as the HA service, has the name of the destination context configured. Use the configuration example below:

**configure**

```
context <context_name>

    ip context-name <context_name>

end
```

Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

## Configuring APN Parameters

This section provides instructions for configuring the APN templates to support Proxy Mobile IP for all IP PDP contexts they facilitate.



**Important:** This is an optional configuration. In addition, attributes returned from the subscriber's profile for non-transparent IP PDP contexts take precedence over the configuration of the APN.

These instructions assume that you are at the root prompt for the Exec mode:

```
[local]host_name#
```

**Step 1** Enter the configuration mode by entering the following command:

```
configure
```

The following prompt appears:

```
[local]host_name(config)#
```

**Step 2** Enter context configuration mode by entering the following command:

```
context <context_name>
```

*context\_name* is the name of the system destination context designated for APN configuration. The name must be from 1 to 79 alpha and/or numeric characters and is case sensitive. The following prompt appears:

```
[<context_name>]host_name(config-ctx)#
```

**Step 3** Enter the configuration mode for the desired APN by entering the following command:

```
apn <apn_name>
```

*apn\_name* is the name of the APN that is being configured. The name must be from 1 to 62 alpha and/or numeric characters and is not case sensitive. It may also contain dots (.) and/or dashes (-). The following prompt appears:

```
[<context_name>]host_name(config-apn)#
```

**Step 4** Enable proxy Mobile IP for the APN by entering the following command:

```
proxy-mip required
```

This command causes proxy Mobile IP to be supported for all IP PDP contexts facilitated by the APN.

**Step 5** *Optional.* GGSN/FA MN-NAI extension can be skipped in MIP Registration Request by entering following command:

```
proxy-mip null-username static-homeaddr
```

This command will enable the accepting of MIP Registration Request without NAI extensions in this APN.

**Step 6** Return to the root prompt by entering the following command:

```
end
```

The following prompt appears:

```
[local]host_name#
```

**Step 7** Repeat *step 1* through *step 6* as needed to configure additional APNs.

**Step 8** Verify that your APNs were configured properly by entering the following command:

```
show apn { all | name <apn_name> }
```

Keyword	Description
	Displays configuration information for all configured APN.

Keyword	Description
	Displays configuration information for the APN with the specified name. apn_name is the name of the APN.

The output is a detailed listing of configured APN parameter settings.

- Step 9** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.



# Appendix Q

## QoS Management

---

This appendix describes the Quality of Service (QoS) management on Cisco® ASR 5000 chassis and explains how it is configured.

The product Administration Guides provide examples and procedures for configuration of basic services on the system. You should select the configuration example that best meets your service model and configure the required elements for that model as described in the respective product Administration Guide, before using the procedures in this appendix.

This appendix describes the following topics:

- [Introduction](#)
- [Dynamic QoS Renegotiation](#)
- [Network Controlled QoS \(NCQoS\)](#)
- [Configuring Dynamic QoS Renegotiation](#)
- [Configuring Network Controlled QoS \(NCQoS\)](#)
- [Monitoring Dynamic QoS Renegotiation Operation](#)

## Introduction

The QoS Traffic Policing functionality supported by the GGSN implements QoS for subscribers based on the configuration of the APN template. As a result, all subscriber PDP contexts using the APN receive the same QoS level. This could lead to unused or under-utilized bandwidth by some subscribers thus reducing the amount of resources available to others.

## Dynamic QoS Renegotiation

Dynamic QoS Renegotiation minimizes the risk of bandwidth mis-appropriation. This feature allows the GGSN to analyze application traffic, and trigger QoS renegotiation with the SGSN to optimize service performance.

In Dynamic QoS Renegotiation, the GGSN performs packet inspection of application traffic to detect the type of service being utilized and automatically renegotiates the QoS to the appropriate level with a maximum QoS level corresponding to the level granted by the HLR.

QoS renegotiation is performed by sending an Update PDP Context Request to the SGSN. This solution is optimal since the appropriate QoS level is always granted to the subscriber without any requirement on the handset or on the core network. The only prerequisite is QoS renegotiation support on the SGSN. In this model, over reservation of radio resources is avoided, while maintaining the appropriate bandwidth for subscribers with real requirements.

The ASR 5000 supports L7 stateful analysis and QoS Renegotiation. These functions combine to become Dynamic QoS Renegotiation. The system also generates CDRs (or real time charging information) that includes the current QoS information and the service accessed. This enables intelligent application-based charging of services, taking into account the granted QoS. It also enables rebates when it was not possible to provide the QoS level required by an application.



**Important:** For L7 traffic analysis an ECSv2 license is required.

## How Dynamic QoS Renegotiation Works

Implementation of Dynamic QoS Renegotiation involves the following:

- Initial QoS
- Service Detection
- Classification of Application Traffic
- Quality of Service Renegotiation

### Initial QoS

When the session is established, an initial level of QoS must be assigned to the subscriber. The GGSN may either grant the requested QoS, or grant a lower QoS level (minimum or intermediate level). The initial QoS remains in effect until the SGSN or GGSN requests a change. When Dynamic QoS Renegotiation is enabled, there are several conditions when the system would request a QoS change.

- Services detected that do not need high QoS: After a configurable time period of a subscriber having terminated services that require high QoS, the system could lower the QoS to a value more appropriate to the services actually being used.
- Services detected that require higher QoS: As soon as a subscriber begins using a service that needs a high QoS, the system immediately attempts to raise the QoS through its service detection capability.

### Service Detection

The Application analysis approach to service detection uses application level (L7) information. In the ASR 5000 chassis, application analysis is stateful—keeping track of the application state.



**Important:** For L7 traffic analysis ECSv2 license is required.

## Classification of Application Traffic

Application traffic can be classified into the following: Conversational, Streaming, Interactive 1, Interactive 2, Interactive 3, or Background. Traffic class can be configured in the charging-action, but it does not take direction as a parameter. However, you can configure a rule matching uplink-only or downlink-only packets and associate it with the charging-action.

QoS renegotiation requires knowing what kind of data packets are flowing through for a particular user to associate a given traffic class with the user's current usage pattern. This is done through packet inspection for a subscriber profile via an Access Control List (ACL). Limits for each traffic class can be configured in the APN. The same infrastructure is reused to perform Dynamic QoS Renegotiation.

After classification of traffic and if required by subscriber profile, Dynamic QoS Renegotiation takes place.

## L4 Packet Inspection

L4 packet analysis has no or low impact on the system performance with very limited impact on system capacity. L4 packet inspection is fully supported by the system.

## L7 Packet Inspection

L7 packet analysis has a greater impact on system performance with very limited impact on the system capacity. L7 packet inspection involves complete application layer analysis and copes with customized applications.

## QoS Renegotiation for a Subscriber QoS Profile

The following is the overall Dynamic QoS Renegotiation process.

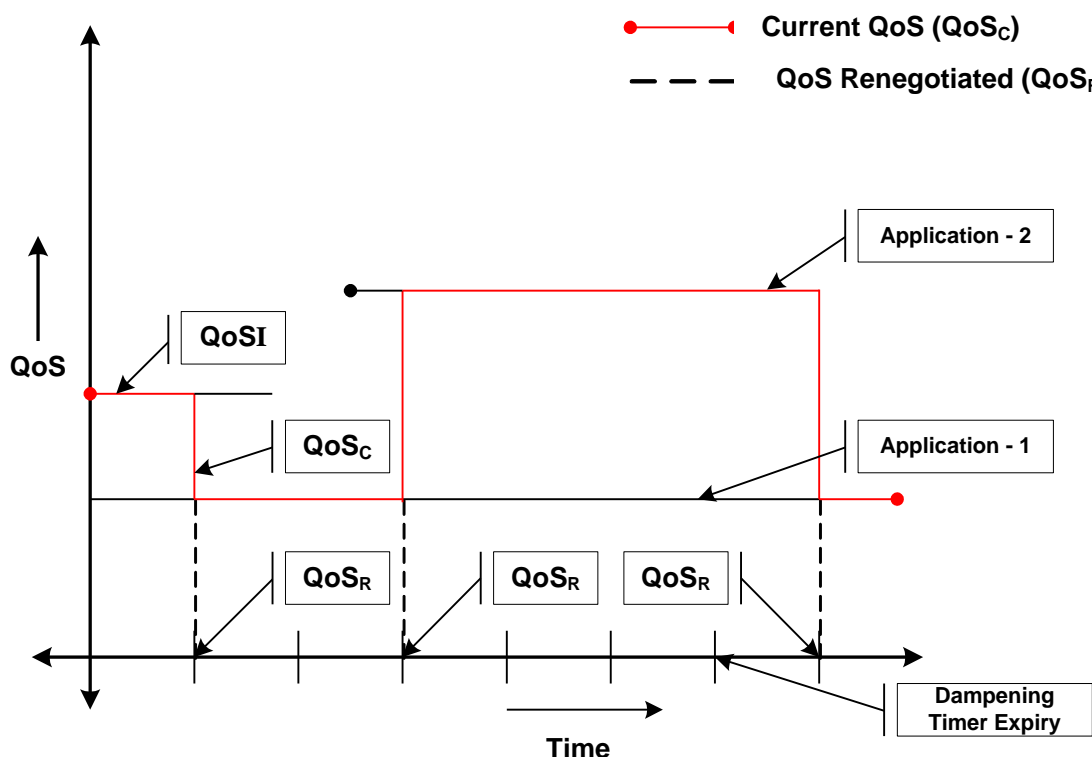
1. When a subscriber attaches to the network, the following happens:
  - Dampening timer is started for the subscriber.
  - QoSI is assigned to the subscriber. This becomes the QoSC till a re-negotiation occurs, as shown in the figure below.
  - The traffic class bitfield is cleared.
2. As the subscriber starts using some applications, the traffic gets classified on the basis of type of data packets or traffic as mentioned in section *Classification of Application Traffic*. The corresponding bit in the Traffic-class-bitfield is set accordingly.
3. The mechanics of QoS renegotiation are as follows:
  - Examine traffic-class-bitfield to determine the highest bit that is set. This gives the desired QoS Traffic Class (QoSD). The associated uplink/downlink peak-data-rate and guaranteed-data-rate values are taken from the configured parameters for this traffic class in the subscriber APN.
  - If QoSC matches QoSD, no QoS renegotiation is required. Otherwise, send an Update PDP Context Request to the SGSN with the QoSD values and QoS renegotiation starts.
  - Reset the dampening timer.
  - Clear the traffic-class-bitfield.
4. QoS renegotiation happens under the following conditions:



- When a higher priority traffic is detected, QoS is renegotiated immediately without waiting for the dampening time to expire. For example, if the current traffic has a QoS of Interactive and the system detects streaming traffic, QoS is immediately upgraded to Streaming.
- When lower priority traffic is detected, the system waits for the expiry of the dampening timer before lowering the QoS.
- During “silence” or no-traffic, QoS renegotiation requests are not initiated.

As seen in the following figure, the QoS profile for the subscriber goes through three renegotiations to match the QoS profile of the highest priority application currently being used.

Figure 83. Dynamic QoS Renegotiation Graph



When there is no traffic, traffic class drops to “Background” and the corresponding QoS profile is negotiated as described above.

## Network Controlled QoS (NCQoS)

Network-controlled QoS is the method by which the system updates the QoS for a PDP context (primary or secondary) upon receipt of Network Requested Update PDP Context (NRUPC) messages from the GGSN. The system can also activate a new secondary PDP context upon receipt of a Network Requested Secondary PDP Context Activation (NRSPCA) message from the GGSN.

### How Network Controlled QoS (NCQoS) Works

The GGSN activates or modifies a bearer whenever a service flow matches a statically provisioned Policy and Charging Control (PCC) rule. The network, based on QoS requirements of the application/service, determines what bearers are needed and either modifies an existing bearer or activates a new one.

Statically provisioned PCC rules, called Network Requested Operation (NRO) rules, are configured as charging rules in the Active Charging Service (ACS). As a part of charging action for such rules, QoS-needed and corresponding Traffic Flow Template (TFT) packet filters are configured. QoS-needed mainly consists of QoS Class Identifier (QCI) and data rates. Whereas, TFT mainly consists of uplink and downlink packet filter information.



**WARNING:** This feature does not work in conjunction with IMS-Authorization service.

When a packet arrives, the ACS analyzes it and performs rule matching based on the priority in the rulebase. If an NRO rule bound to the context on which the packet arrived matches, ACS applies the bandwidth limit and gating. If an NRO rule bound to some other context matches, ACS discards the packet.

If an unbound NRO rule matches, ACS finds a context with the same QCI as the NRO rule, where the context's Maximum Bit Rate (MBR) and matched rule's MBR (context's MBR + matched rule's MBR) is less than the MBR for that QCI in the APN. If such a context is found, NRUPC for that context is triggered. If the request succeeds, the rule will be bound to that context.



**Important:** The packet that triggered the NRUPC request is discarded.

If no context satisfying the MBR limit is found, or if there is no context with the same QCI as the NRO rule, the system triggers NRSPCA. If the request succeeds, the rule is bound to that context.



**Important:** The packet that triggered the NRSPCA request is discarded.

TFTs from the charging-action associated with the NRO rule are also sent as part of the NRUPC/NRSPCA request, and returned as part of the Create PDP Context Response.

Finally, if a non-NRO rule matches, ACS proceeds with the normal processing of that packet. Non-NRO charging-actions can still do “flow action” or ITC (limit-for-flow-type and limit-for-bandwidth).

ACS also does the following:

- Before making an NRUPC/NRSPCA Request, ACS checks if there is any outstanding request for the same QCI for the same subscriber. If there is, it will not process the new request and discards the packet.
- After a context is terminated, ACS unbinds all the rules bound to that context. Such a rule can later be bound to some other context when a packet matches that rule.



---

**Important:** The packet that triggered the NRUPC/NRSPCA request is discarded.

---

## Configuring Dynamic QoS Renegotiation

This section describes how to configure per-APN based Dynamic QoS Renegotiation.



**Caution:** For Dynamic QoS Renegotiation, two RADIUS attributes are required for remote subscriber configuration. For a particular subscriber, these attributes can be overridden without considering the timeout for Dynamic QoS Renegotiation and whether Dynamic QoS Renegotiation is enabled or not.

To configure Dynamic QoS Renegotiation:

- Step 1** Configure an Access Control List (ACL), as described in the [Configuring ACL for Dynamic QoS Renegotiation](#) section.
- Step 2** Configure an APN for Dynamic QoS Renegotiation as described in the [Configuring APNs for Dynamic QoS Renegotiation](#) section.
- Step 3** Save your configuration as described in the *Verifying and Saving Your Configuration* chapter in this guide.
- Step 4** Monitor the operations as described in the [Monitoring Dynamic QoS Renegotiation Operation](#) section.



**Important:** Commands used in the configuration examples in this section reflect base functionality (most common or likely commands and/or keyword options). In many cases, other commands and/or keyword options are available. Refer to the *ACS Configuration Mode Commands* and *APN Configuration Mode Commands* sections of the *Command Line Interface Reference* for complete information regarding all commands.

## Configuring ACL for Dynamic QoS Renegotiation

Configuring an ACL and applying it to an APN template are required to specify permission and treatment levels for Dynamic QoS Renegotiation.

Use the following example to configure an ACL for Dynamic QoS Renegotiation:

```
configure

context <context_name>

    ip access-list <acl_name>

        permit { tcp | udp } ..... treatment { background | conversational |
interactive-1 | interactive-2 | interactive-3 | streaming }

    end
```

Notes:

- *context\_name* must be the name of the destination context in which you want to configure the ACL. The same context must be used for APN configuration.
- For information on configuring the rules that comprise the ACL, refer to the *Access Control Lists* appendix.

## Configuring Charging Action for Dynamic QoS Renegotiation

Use the following example to configure charging action parameters for Dynamic QoS Renegotiation support:

```
configure

  active-charging service <service_name>

    charging-action <charging_action_name> -noconfirm

    qos-renegotiate traffic-class streaming

    flow action discard

    flow limit-for-bandwidth direction downlink peak-data-rate <bps> peak-
burst-size <bytes> violate-action lower-ip-precedence

  end
```

Notes:

- A maximum of eight packet filters can be configured per charging action.
- The flow limit-for-bandwidth command contains other option than the example shown here. Refer ti the *ACS Charging Action Configuration Mode Commands* chapter in the *Command Line Interface Reference* for more information on this command.

## Configuring Rulebase for Dynamic QoS Renegotiation

Use the following example to configure rulebase parameters for Dynamic QoS Renegotiation support:

```
configure

  active-charging service <service_name>

    rulebase <rulebase_name> [ -noconfirm ]

    qos-renegotiate timeout <timeout>

  end
```

## Configuring APNs for Dynamic QoS Renegotiation

Use the following example to configure an APN template's QoS profile in support of Dynamic QoS Renegotiation:

```
configure

  context <context_name>

    apn <apn_name>

    ip access-group <acl_name> [ in | out ]
```

**end**

Notes:

- *context\_name* must be the name of the destination context in which you have already configured the ACL, and want to configure the APN template.
- *<acl\_name>* must be the name of the ACL that you have already configured in the context.
- If the optional **in** or **out** keywords are not specified in the **ip access-group** command (APN Configuration Mode), the ACL will be applied to all inbound and outbound packets.

## Configuring Network Controlled QoS (NCQoS)

To configure NCQoS:

- Step 1** Configure packet filter parameters as described in the [Configuring Packet Filter for NCQoS](#) section.
- Step 2** Configure charging rules and actions as described in the [Configuring Charging Action for NCQoS](#) section.
- Step 3** Configure APN template and enable bearer control mode for NCQoS as described in the [Configuring APN for NCQoS](#) section.
- Step 4** Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.
- Step 5** Monitor the operations as described in the [Monitoring Dynamic QoS Renegotiation Operation](#) section.



**Important:** Commands used in the configuration examples in this section implement base functionality (most common or likely commands and/or keyword options). In many cases, other commands and/or keyword options are available. Refer to the *Command Line Interface Reference* for complete information regarding all commands.

### Configuring Packet Filter for NCQoS

Use the following example to configure packet filter parameters for NCQoS support:

```
configure

active-charging service <service_name>

    packet-filter <filter_name> [ -noconfirm ]

        ip local-port { = <port_num> | range <start_port_num> to <end_port_num> }

        ip protocol { = <proto_num> | range <start_proto_num> to <end_proto_num> }

        ip remote-address { = { <ip_address> | <ip_address/mask> } | { range {
<ip_address> | <ip_address/mask> } to { <ip_address> | <ip_address/mask> } }

        ip remote-port { = <port_num> | range <start_port_num> to <end_port_num> }

        direction { bi-directional | download | upload }

        priority <priority>

    end
```

### Configuring Charging Action for NCQoS

Use the following example to configure charging action parameters for NCQoS support:

```

configure

  active-charging service <service_name>

    charging-action <charging_action_name> [ -noconfirm ]

    qos-class-identifier <identifier>

    flow action discard [ downlink | uplink ]

    tft packet-filter <filter_name>

    flow limit-for-bandwidth direction { downlink | uplink } peak-data-rate <bps>
peak-burst-size <bytes> violate-action { discard | lower-ip-precedence }

  end

```

Notes:

- A number of optional keywords and variable are available for the **flow limit-for-bandwidth direction** command. Refer to the *ACS Charging Action Configuration Mode Commands* section of the *Command Line Interface Reference* for more information regarding this command.

## Configuring APN for NCQoS

Use the following example to enable Bearer Control Mode (BCM) for NCQoS support:

```

configure

  context <context_name>

    apn <apn_name>

    bearer-control-mode [ mixed | ms-only | none ]

  end

```

Notes:

- To enable NCQoS, bearer-control-mode in the APN Configuration Mode must be configured with **mixed** mode.



# Monitoring Dynamic QoS Renegotiation Operation

Use the following steps to verify/monitor Dynamic QoS Renegotiation operations:

**Step 1** Verify that your APNs were configured properly by entering the following command:

```
show apn { all | name apn_name }
```

The output is a listing of APN parameter settings.

**Step 2** Verify that the ACLs have been properly applied by entering the following command:

```
show apn name apn_name
```

*apn\_name* must be the name of the APN configured in the *Configuring APNs for Dynamic QoS Renegotiation* section. The output of this command displays the APN configuration. Examine the output for the **ip output access-group** and **ip input access-group** fields. For more details refer to the *Applying a Single ACL to Multiple Subscribers* section.

**Step 3** Verify that your ACL was configured properly by entering the following command:

```
show ip access-list acl_name
```

The output is a concise listing of IP Access Control List parameter settings.

**Step 4** Monitor your QoS renegotiation status for a subscriber by running the **show subscriber ggsn-only full** command (Exec mode).

The output is a concise listing of subscribers' settings.

**Step 5** For L7 based QoS Renegotiation, view how many time QoS renegotiations have happened for that session by running the **show active-charging sessions full all** command (Exec mode).

**Step 6** View the statistics of APN related to QoS renegotiation parameters by entering the following command:

```
show apn statistics { all | name apn_name }
```

The output is a listing of APN statistics related to QoS Renegotiation.

## Event IDs Pertaining to Dynamic QoS Renegotiation

The Session Manager facility sources event IDs that can be useful for diagnosing errors that could occur when implementing of Dynamic QoS Renegotiation feature.

The following table displays information pertaining to these events.

**Table 45. Event IDs in Session Manager Pertaining to Dynamic QoS Renegotiation**

Event	Event ID	Type	Additional Information
-------	----------	------	------------------------

Event	Event ID	Type	Additional Information
QoS Renegotiation timer started for subscriber	10917	Info	“Indicates that the Dynamic QoS Renegotiation timer was started for the subscriber”
QoS Renegotiation timer stopped for subscriber	10918	Info	“Indicates that the Dynamic QoS Renegotiation timer was stopped for the subscriber”
QoS Renegotiation timer expired for subscriber	10919	Info	“Indicates that the Dynamic QoS Renegotiation timer was expired for the subscriber”
QoS Renegotiation message sent for subscriber	10920	Info	“Indicates that the Dynamic QoS Renegotiation message was sent for the subscriber”
L4 classification done for subscriber traffic	10921	Info	“Indicates the kind of L4 classification that was done for the subscriber traffic.”

## RADIUS Attributes

The RADIUS attributes listed in the following table are used to enable Dynamic QoS Renegotiation for subscribers configured on remote RADIUS servers. More information on these attributes can be found in the *AAA and GTPP Interface Administration and Reference*.

**Table 46. RADIUS Attributes Required for Dynamic QoS Renegotiation Support**

Attribute	Description
SN-Enable-QoS-Renegotiation (or SN1-Enable-QoS-Renegotiation)	Enables the Dynamic QoS Renegotiation for specific profile application. This attribute displays “enable qos renegotiation”.
SN-QoS-Renegotiation-Timeout (or SN1-QoS-Renegotiation-Timeout)	Timeout duration for dampening time for QoS renegotiation to specific profile application. This attribute displays “qos renegotiation timeout”.

# Appendix R

## Remote Address-based RADIUS Accounting

---

This chapter provides information on configuring an enhanced, or extended, service. The product administration guides provide examples and procedures for the configuration of basic services on the system. It is recommended that you select the configuration example that best meets your service model, and configure the required elements for that model before using the procedures in this chapter.

This chapter includes the following sections:

- [Overview](#)
- [Configuring Remote Address-based Accounting](#)
- [Subscriber Attribute Configuration](#)

## Overview

Remote address-based RADIUS accounting counts the number of octets exchanged between individual subscribers and specific remote IP addresses, or networks, during a packet data session. Data from the subscriber to the remote addresses, and data from the remote addresses to the subscriber are accounted for separately.

The remote addresses for which to collect RADIUS accounting data are configured in lists on a per-context basis. Individual subscribers are associated with particular address lists through the configuration or specification of an attribute in their locally configured or RADIUS server-based profiles. Once the lists and subscriber profiles are configured, accounting data collection can be enabled on the system.

Remote address-based RADIUS accounting is implemented in the system according to the specifications described in TIA/EIA/IS-835-B, CDMA2000 Wireless IP Network Standard, October 2002 and 3GPP2 X.S0011-005-D.

## License Requirements

The Remote address-based RADIUS Accounting is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the Managing License Keys section of the Software Management Operations chapter in the *System Administration Guide*.

## Configuring Remote Address-based Accounting

To configure this functionality, a list of up to ten remote addresses or networks is configured in the authentication context, the list is assigned to a subscriber, and remote address collection is enabled.

Use the following configuration example to configure remote address-based accounting:

```
configure

context <context_name>

    radius group <group_name>

    radius accounting ip remote-address list <list_id>

    address <ipv4_address/ipv6_address> netmask <netmask>

end
```

## Verifying the Remote Address Lists

Use the following command to verify the remote address lists:

```
show configuration context <context_name>
```

Output similar to the following is displayed.

```
[local] host_name # show configuration context <context_name>
```

```
configure

context <context_name>

    subscriber default

    exit

radius accounting ip remote-address list 1

    address <ipv4_address/ipv6_address> netmask <netmask>

    address <ipv4_address/ipv6_address> netmask <netmask>

    address <ipv4_address/ipv6_address> netmask <netmask>

end
```

Notes:

- Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

## Subscriber Attribute Configuration

Subscriber attributes are configured as part of their profile. Subscriber profiles can be configured either remotely on a RADIUS server or locally on the system.

This section provides information and procedures on the attributes used to support this functionality.



**Important:** Since the instructions for configuring subscribers differ between RADIUS server applications, this section only provides the individual attributes that can be added to the subscriber profile. Please refer to the documentation that shipped with your RADIUS server for instructions on configuring subscribers.

## Supported RADIUS Attributes

The following RADIUS attributes are used to configure remote address-based RADIUS accounting for a subscriber session. For specific information on each attribute, see the *AAA and GTPP Interface Administration and Reference*.

- 3GPP2-Remote-Addr-Table-Index
- 3GPP2-Remote-IPv4-Address
- 3GPP2-Remote-IPv4-Addr-Octets

## Configuring Local Subscriber Profiles

Use the following example to configure local subscriber profiles to support the Remote Address-based RADIUS Accounting feature:

```
configure
```

```
    context <context_name>
```

```
        subscriber name <name>
```

```
            radius accounting ip remote-address list-id <list_id>
```

```
        end
```

```
configure
```

```
    context <context_name>
```

```
        radius accounting ip remote-address collection
```

```
    end
```

Notes:

- Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.







# Appendix S

## Subscriber Overcharging Protection

---

Subscriber Overcharging Protection is a proprietary, enhanced feature that prevents subscribers in UMTS networks from being overcharged when a loss of radio coverage (LORC) occurs. This chapter indicates how the feature is implemented on various systems and provides feature configuration procedures. Products supporting subscriber overcharging protection include Cisco's Gateway GPRS Support Node (GGSN) and Serving GPRS Support Node (SGSN).

The individual product administration guides provide examples and procedures for configuration of basic services. Before using the procedures in this chapter, we recommend that you select the configuration example that best meets your service model, and configure the required elements for that model, as described in the respective guide.



**Important:** Subscriber Overcharging Protection is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

---

This chapter covers the following topics in support of the Subscriber Overcharging Protection feature:

- [Feature Overview](#)
- [Overcharging Protection - GGSN Configuration](#)
- [Overcharging Protection - SGSN Configuration](#)

## Feature Overview

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

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

Previously, upon loss of radio coverage (LORC), the SGSN did not perform the UPC procedure to set QoS to 0kbps, as it does when the traffic class is either streaming or conversational. Therefore, when the SGSN did a Paging Request, if the mobile did not respond the SGSN would simply drop the packets without notifying the GGSN; the G-CDR would have increased counts but the S-CDR would not, causing overcharges when operators charged the subscribers based on the G-CDR.

Now operators can accommodate this situation, they can configure the SGSN to set QoS to 0kbps, or to a negotiated value, upon detecting the loss of radio coverage. The overcharging protection feature relies upon the SGSN adding a proprietary private extension to GTP LORC Intimation IE to messages. This LORC Intimation IE is included in UPCQ, DPCQ, DPCR, and SGSN Context Response GTP messages. One of the functions of these messages is to notify the GGSN to prevent overcharging.

The GGSN becomes aware of the LORC status by recognizing the message from the SGSN and discards the downlink packets if LORC status indicates loss of radio coverage or stops discarding downlink packets if LORC status indicates gain of radio coverage for the UE.

The following table summarizes the SGSN's actions when radio coverage is lost or regained and LORC overcharging protection is enabled.

**Table 47. LORC Conditions and Overcharging Protection**

Condition	Triggered by	SGSN Action	LORC Intimation IE - private extension payload
Loss of radio coverage (LORC)	RNC sends Iu release request with cause code matching configured value	Send UPCQ to GGSN Start counting unsent packets/bytes Stop forwarding packets in downlink direction	No payload
Mobile regains coverage in same SGSN area	MS/SGSN	Send UPCQ to GGSN Stop counting unsent packets/bytes Stop discarding downlink packets	New loss-of-radio-coverage state and unsent packet/byte counts
Mobile regains coverage in different SGSN area	MS/SGSN	Send SGSN Context Response message to new SGSN Stop counting unsent packets/bytes	Unsent packet/byte counts
PDP deactivated during LORC	MS/SGSN	Send DPCQ to GGSN Stop counting unsent packets/bytes	Unsent packet/byte counts

Condition	Triggered by	SGSN Action	LORC Intimation IE - private extension payload
PDP deactivated during LORC	GGSN	Send DPCR to GGSN Stop counting unsent packets/bytes	Unsent packet/byte counts

## Overcharging Protection - GGSN Configuration

This section provides a high-level series of steps and the associated configuration examples for configuring the GGSN to support subscriber overcharging protection.



**Important:** This section provides the minimum instruction set to configure the GGSN to avoid the overcharging due to loss of radio coverage in UMTS network. For this feature to be operational, you must also implement the configuration indicated in the section *Overcharging Protection - SGSN Configuration* also in this chapter. Commands that configure additional function for this feature are provided in the *Cisco ASR 5000 Command Line Interface Reference*.

These instructions assume that you have already configured the system-level configuration as described in *Cisco ASR 5000 System Administration Guide* and the *Cisco ASR 5000 Gateway GPRS Support Node Administration Guide*.

To configure the system to support overcharging protection on LORC in the GGSN service:

- Step 1** Configure the GTP-C private extension in a GGSN service by applying the example configurations presented in the *GTP-C Private Extension Configuration* section below.
- Step 2** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.
- Step 3** Verify configuration of overcharging protection on LORC related parameters by applying the commands provided in the *Verifying Your GGSN Configuration* section in this chapter.

### GTP-C Private Extension Configuration

This section provides the configuration example to configure the GTP-C private extensions for GGSN service:

```
configure

context <vpn_context_name>

    ggsn-service <ggsn_svc_name>

        gtpc private-extension loss-of-radio-coverage

    end
```


Notes:

- <vpn\_context\_name> is the name of the system context where specific GGSN service is configured. For more information, refer *Cisco ASR 5000 Gateway GPRS Support Node Administration Guide*.
- <ggsn\_svc\_name> is name of the GGSN service where you want to enable the overcharging protection for subscribers due to LORC.

## Verifying Your GGSN Configuration

This section explains how to display and review the configurations after saving them in a *.cfg* file (as described in the *Verifying and Saving Your Configuration* chapter in this book) and how to retrieve errors and warnings within an active configuration for a service.

---

 **Important:** All commands listed here are under Exec mode. Not all commands are available on all platforms.

---

These instructions are used to verify the overcharging protection support configuration.

**Step 1** Verify that your overcharging support is configured properly by entering the following command in Exec Mode:

```
show ggsn-service name ggsn_svc_name
```

The output of this command displays the configuration for overcharging protection configured in the GGSN service *ggsn\_svc\_name*.

```
Service name:                ggsn_svc1
Context:                     service
Accounting Context Name:service
Bind:                        Done
Local IP Address:            192.169.1.1    Local IP Port:    2123
...
...
GTP Private Extensions:
    Preservation Mode
    LORC State
```

**Step 2** Verify that GTP-C private extension is configured properly for GGSN subscribers by entering the following command in Exec Mode:

```
show subscribers ggsn-only full
```

The output of this command displays the LORC state information and number of out packets dropped due to LORC.

## Overcharging Protection - SGSN Configuration

This section provides a high-level series of steps and the associated configuration examples for configuring the SGSN to support subscriber overcharging protection.



**Important:** This section provides a minimum instruction set to configure the SGSN to implement this feature. For this feature to be operational, you must also implement the configuration indicated in the section *Overcharging Protection - GGSN Configuration* also in this chapter.

Command details can be found in the *Cisco ASR 5000 Command Line Interface Reference*.

These instructions assume that you have already completed:

- the system-level configuration as described in the *Cisco ASR 5000 System Administration Guide*,
- the SGSN service configuration as described in the *Cisco ASR 5000 Serving GPRS Support Node Administration Guide*, and
- the configuration of an APN profile as described in the *Operator Policy* chapter in this guide.

To configure the SGSN to support subscriber overcharging protection:

- Step 1** Configure the private extension IE with LORC in an APN profile by applying the example configurations presented in the *Private Extension IE Configuration* section.



**Important:** An APN profile is a component of the Operator Policy feature implementation. To implement this feature, an APN profile must be created and *associated* with an operator policy. For details, refer to the *Operator Policy* chapter in this book.

- Step 2** Configure the RANAP cause that should trigger this UPCQ message by applying the example configurations presented in the *RANAP Cause Trigger Configuration* section.
- Step 3** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.
- Step 4** Verify the SGSN portion of the configuration for overcharging protection on LORC related parameters by applying the commands provided in the *Verifying the Feature Configuration* section.

### Private Extension IE Configuration

This section provides the configuration example to enable adding the private extension IE that will be included in the messages sent by the SGSN when a loss of radio coverage occurs in the UMTS network:

```
configure

apn-profile <apn_profile_name>

    gtp private-extension loss-of-radio-coverage send-to-ggsn

end
```

Note:

- `<apn_profile_name>` is the name of a previously configured APN profile. For more information, refer to the *Operator Policy* chapter, also in this book.

## RANAP Cause Trigger Configuration

This section provides the configuration example to enable the RANAP cause trigger and define the trigger message value:

```
configure

context <context_name>

    iups-service <iups_service_name>

        loss-of-radio-coverage ranap-cause <cause>          end
```

Note:

- `<context_name>` is the name of the previously configured context in which the IuPS service has been configured.
- `<cause>` is an integer from 1 to 512 (the range of reasons is a part of the set defined by 3GPP TS 25.413) that allows configuration of the RANAP Iu release cause code to be included in messages. Default is 46 (MS/UE radio connection lost).

## Verifying the Feature Configuration

This section explains how to display the configurations after saving them in a `.cfg` file as described in the *Verifying and Saving Your Configuration* chapter elsewhere in this guide.



**Important:** All commands listed here are under Exec mode. Not all commands are available on all platforms.

These instructions are used to verify the overcharging protection support configuration.

**Step 1** Verify that your overcharging support is configured properly by entering the following command in Exec Mode:

```
show apn-profile full name apn_profile_name
```

The output of this command displays the entire configuration for the APN profile configuration. Only the portion related to overcharging protection configuration in the SGSN is displayed below. Note that the profile name is an example:

```
APN Profile name:                : apnprofile1

Resolution Priority:              : dns-fallback

...

...
```

```
Sending Private Extension Loss of Radio Coverage IE

To GGSN                               : Enabled

To SGSN                               : Enabled
```

**Step 2** Verify the RANAP Iu release cause configuration by entering the following command in the Exec Mode:

```
show iups-service name <iups_service_name>
```

The output of this command displays the entire configuration for the IuPS service configuration. Only the portion related to overcharging protection configuration (at the end of the display) is displayed below. Note that the IuPS service name is an example:

```
Service name:                          : iups1

Service-ID:                            : 1

...

...

Loss of Radio Coverage

Detection Cause in Iu Release: 46
```



# Appendix T

## Traffic Policing and Shaping

---

This chapter describes the support of per subscriber Traffic Policing and Shaping feature on Cisco's Chassis and explains the commands and RADIUS attributes that are used to implement this feature. The product Administration Guides provide examples and procedures for configuration of basic services on the system. It is recommended that you select the configuration example that best meets your service model, and configure the required elements for that model, as described in the respective product Administration Guide, before using the procedures in this chapter.



**Important:** Traffic Policing and Shaping is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

---

This chapter included following procedures:

- [Overview](#)
- [Traffic Policing Configuration](#)
- [Traffic Shaping Configuration](#)
- [RADIUS Attributes](#)

## Overview

This section describes the traffic policing and shaping feature for individual subscriber. This feature is comprised of two functions:

- Traffic Policing
- Traffic Shaping

## Traffic Policing

Traffic policing enables the configuring and enforcing of bandwidth limitations on individual subscribers and/or APN of a particular traffic class in 3GPP/3GPP2 service.

Bandwidth enforcement is configured and enforced independently on the downlink and the uplink directions.

A Token Bucket Algorithm (a modified trTCM) [RFC2698] is used to implement the Traffic-Policing feature. The algorithm used measures the following criteria when determining how to mark a packet:

- **Committed Data Rate (CDR):** The guaranteed rate (in bits per second) at which packets can be transmitted/received for the subscriber during the sampling interval.
- **Peak Data Rate (PDR):** The maximum rate (in bits per second) that subscriber packets can be transmitted/received for the subscriber during the sampling interval.
- **Burst-size:** The maximum number of bytes that can be transmitted/received for the subscriber during the sampling interval for both committed (CBS) and peak (PBS) rate conditions. This represents the maximum number of tokens that can be placed in the subscriber's "bucket". Note that the committed burst size (CBS) equals the peak burst size (PBS) for each subscriber.

The system can be configured to take any of the following actions on packets that are determined to be in excess or in violation:

- **Drop:** The offending packet is discarded.
- **Transmit:** The offending packet is passed.
- **Lower the IP Precedence:** The packet's ToS bit is set to "0", thus downgrading it to Best Effort, prior to passing the packet. Note that if the packet's ToS bit was already set to "0", this action is equivalent to "Transmit".

## Traffic Shaping

Traffic Shaping is a rate limiting method similar to the Traffic Policing, but 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.


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.


# Traffic Policing Configuration

Traffic Policing is configured on a per-subscriber basis. The subscribers can either be locally configured subscribers on the system or subscriber profiles configured on a remote RADIUS server.

In 3GPP service Traffic policing can be configured for subscribers through APN configuration as well.

---


 **Important:** In 3GPP service attributes received from the RADIUS server supersede the settings in the APN.

 **Important:** Commands used in the configuration samples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the *Command Line Interface Reference* for complete information regarding all commands.

---

## Configuring Subscribers for Traffic Policing

---

 **Important:** Instructions for configuring RADIUS-based subscriber profiles are not provided in this document. Please refer to the documentation supplied with your server for further information.

---

**Step 1** Configure local subscriber profiles on the system to support Traffic Policing by applying the following example configurations:

**Step a.....** To apply the specified limits and actions to the downlink (data to the subscriber):

```
configure
context <context_name>
    subscriber name <user_name>
        qos traffic-police direction downlink
    end
```

**Step b .....** To apply the specified limits and actions to the uplink (data from the subscriber):

```
configure
context <context_name>
    subscriber name <user_name>
        qos traffic-police direction uplink
    end
```

Notes:

- There are numerous keyword options associated with the **qos traffic-police direction { downlink | uplink }** command.
- Repeat for each additional subscriber to be configured.



**Important:** If the exceed/violate action is set to “lower-ip-precedence”, the TOS value for the outer packet becomes “best effort” for packets that exceed/violate the traffic limits regardless of what the **ip user-datagram-tos-copy** command in the Subscriber Configuration mode is configured to. In addition, the “lower-ip-precedence” option may also override the configuration of the **ip qos-dscp** command (also in the Subscriber Configuration mode). Therefore, it is recommended that command not be used when specifying this option.

**Step 2** Verify the subscriber profile configuration by applying the following example configuration:

```
context <context_name>

show subscriber configuration username <user_name>
```

**Step 3** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

## Configuring APN for Traffic Policing in 3GPP Networks

This section provides information and instructions for configuring APN template’s QoS profile in support of Traffic Policing.

The profile information is sent to the SGSN(s) in response to GTP Create/Update PDP Context Request messages. If the QoS profile requested by the SGSN is lower than the configured QoS profile configured, the profile requested by the SGSN is used. If the QoS profile requested by the SGSN is higher, the configured rates are used.

Note that values for the committed-data-rate and peak-data-rate parameters are exchanged in the GTP messages between the GGSN and the SGSN. Therefore, the values used may be lower than the configured values. When negotiating the rate with the SGSN(s), the system convert this to a value that is permitted by GTP as shown in the table below.

**Table 48. Permitted Values for Committed and Peak Data Rates in GTP Messages**

Value (bps)	Increment Granularity (bps)
From 1000 to 63,000	1,000 (e.g 1000, 2000, 3000, ... 63000)
From 64,000 to 568,000	8,000 (e.g. 64000, 72000, 80000, ... 568000)
From 576,000 to 8,640,000	64,000 (e.g. 576000, 640000, 704000, ... 86400000)
From 8,700,000 to 16,000,000	100,000 bps (e.g. 8700000, 8800000, 8900000, ... 16000000)

**Step 1** Set parameters by applying the following example configurations:

**Step a**.....To apply the specified limits and actions to the downlink (the Gn direction):

```
configure
```

```

context <context_name>

  apn <apn_name>

  qos rate-limit downlink

end

```

**Step b** ..... To apply the specified limits and actions to the uplink (the Gi direction):

```

configure

context <context_name>

  apn <apn_name>

  qos rate-limit uplink

end

```

Notes:

- There are numerous keyword options associated with **qos rate-limit { downlink | uplink }** command.
- *Optionally*, configure the maximum number of PDP contexts that can be facilitated by the APN to limit the APN's bandwidth consumption by entering the following command in the configuration:

```

max-contents primary <number> total <total_number>

```

- Repeat as needed to configure additional Qos Traffic Policing profiles.



**Important:** If a “subscribed” traffic class is received, the system changes the class to background and sets the following: The uplink and downlink guaranteed data rates are set to 0. If the received uplink or downlink data rates are 0 and traffic policing is disabled, the default of 64 kbps is used. When enabled, the APN configured values are used. If the configured value for downlink max data rate is larger than can fit in an R4 QoS profile, the default of 64 kbps is used. If either the received uplink or downlink max data rates is non-zero, traffic policing is employed if enabled for the background class. The received values are used for responses when traffic policing is disabled.

**Step 2** Verify that your APNs were configured properly by entering the following command:

```

show apn { all | name <apn_name> }

```

The output is a concise listing of configured APN parameter settings.

**Step 3** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

# Traffic Shaping Configuration

Traffic Shaping is configured on a per-subscriber basis. The subscribers can either be locally configured subscribers on the system or subscriber profiles configured on a remote RADIUS server.

In 3GPP service Traffic policing can be configured for subscribers through APN configuration as well.



**Important:** In 3GPP, service attributes received from the RADIUS server supersede the settings in the APN.



**Important:** Commands used in the configuration samples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the *Command Line Interface Reference* for complete information regarding all commands.

## Configuring Subscribers for Traffic Shaping

This section provides information and instructions for configuring local subscriber profiles on the system to support Traffic Shaping.



**Important:** Instructions for configuring RADIUS-based subscriber profiles are not provided in this document. Please refer to the documentation supplied with your server for further information.

**Step 1** Set parameters by applying the following example configurations:

**Step a**.....To apply the specified limits and actions to the downlink (data to the subscriber):

```
configure
context <context_name>
subscriber name <user_name>
qos traffic-shape direction downlink
end
```

**Step b**.....To apply the specified limits and actions to the uplink (data to the subscriber):

```
configure
context <context_name>
subscriber name <user_name>
qos traffic-shape direction uplink
end
```

Notes:

- There are numerous keyword options associated with **qos traffic-shape direction { downlink | uplink }** command.
- Repeat for each additional subscriber to be configured.



**Important:** If the exceed/violate action is set to “lower-ip-precedence”, the TOS value for the outer packet becomes “best effort” for packets that exceed/violate the traffic limits regardless of what the **ip user-datagram-tos-copy** command in the Subscriber Configuration mode is configured to. In addition, the “lower-ip-precedence” option may also override the configuration of the **ip qos-dscp** command (also in the Subscriber Configuration mode). Therefore, it is recommended that command not be used when specifying this option.

**Step 2** Verify the subscriber profile configuration by applying the following example configuration:

```
context <context_name>

show subscriber configuration username <user_name>
```

**Step 3** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

## Configuring APN for Traffic Shaping in 3GPP Networks

This section provides information and instructions for configuring APN template’s QoS profile in support of Traffic Shaping.

The profile information is sent to the SGSN(s) in response to GTP Create/Update PDP Context Request messages. If the QoS profile requested by the SGSN is lower than the configured QoS profile configured, the profile requested by the SGSN is used. If the QoS profile requested by the SGSN is higher, the configured rates are used.

Note that values for the committed-data-rate and peak-data-rate parameters are exchanged in the GTP messages between the GGSN and the SGSN. Therefore, the values used may be lower than the configured values. When negotiating the rate with the SGSN(s), the system convert this to a value that is permitted by GTP as shown in the following table.

**Table 49. Permitted Values for Committed and Peak Data Rates in GTP Messages**

Value (bps)	Increment Granularity (bps)
From 1000 to 63,000	1,000 (e.g 1000, 2000, 3000, ... 63000)
From 64,000 to 568,000	8,000 (e.g. 64000, 72000, 80000, ... 568000)
From 576,000 to 8,640,000	64,000 (e.g. 576000, 640000, 704000, ... 86400000)
From 8,700,000 to 16,000,000	100,000 bps (e.g. 8700000, 8800000, 8900000, ... 16000000)

**Step 1** Set parameters by applying the following example configurations.

**Step a.....** To apply the specified limits and actions to the downlink (data to the subscriber):

```
configure
```

```

context <context_name>

    subscriber name <user_name>

    qos rate-limit downlink

end

```

**Step b.....**To apply the specified limits and actions to the uplink (data to the subscriber):

```

configure

context <context_name>

    apn <apn_name>

    qos rate-limit uplink

end

```

**Step 2** *Optional.* Configure the maximum number of PDP contexts that can be facilitated by the APN to limit the APN's bandwidth consumption by entering the following command in the configuration:

```

configure

context <context_name>

    apn <apn_name>

    max-contexts primary <number> total <total_number>

end

```

Notes:

- There are numerous keyword options associated with **qos rate-limit direction { downlink | uplink }** command.
- For more information on commands, refer *Command Line Interface Reference*
- If the exceed/violate action is set to **lower-ip-precedence**, this command may override the configuration of the **ip qos-dscp** command in the GGSN service configuration mode for packets from the GGSN to the SGSN. In addition, the GGSN service **ip qos-dscp** command configuration can override the APN setting for packets from the GGSN to the Internet. Therefore, it is recommended that command not be used in conjunction with this action.
- Repeat as needed to configure additional Qos Traffic Policing profiles.
- Note that, if a “subscribed” traffic class is received, the system changes the class to background and sets the following:
  - The uplink and downlink guaranteed data rates are set to 0.
  - If the received uplink or downlink data rates are 0 and traffic policing is disabled, the default of 64 kbps is used. When enabled, the APN configured values are used.
  - If the configured value for downlink max data rate is larger than can fit in an R4 QoS profile, the default of 64 kbps is used.



- If either the received uplink or downlink max data rates is non-zero, traffic policing is employed if enabled for the background class. The received values are used for responses when traffic policing is disabled.

**Step 3** Verify that your APNs were configured properly by entering the following command:

```
show apn { all | name <apn_name> }
```

The output is a concise listing of configured APN parameter settings.

**Step 4** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

# RADIUS Attributes

## Traffic Policing for CDMA Subscribers

The RADIUS attributes listed in the following table are used to configure Traffic Policing for CDMA subscribers (PDSN, HA) configured on remote RADIUS servers. More information on these attributes can be found in the *AAA Interface Administration and Reference*.

**Table 50. RADIUS Attributes Required for Traffic Policing Support for CDMA Subscribers**

Attribute	Description
SN-QoS-Tp-Dnlk (or SN1-QoS-Tp-Dnlk)	Enable/disable traffic policing in the downlink direction.
SN-Tp-Dnlk-Committed-Data-Rate (or SN1-Tp-Dnlk-Committed-Data-Rate)	Specifies the downlink committed-data-rate in bps.
SN-Tp-Dnlk-Peak-Data-Rate (or SN1-Tp-Dnlk-Committed-Data-Rate)	Specifies the downlink peak-data-rate in bps.
SN-Tp-Dnlk-Burst-Size (or SN1-Tp-Dnlk-Burst-Size)	Specifies the downlink-burst-size in bytes. <b>NOTE:</b> It is recommended that this parameter be configured to at least the greater of the following two values: 1) 3 times greater than packet MTU for the subscriber connection, OR 2) 3 seconds worth of token accumulation within the “bucket” for the configured peak-data-rate.
SN-Tp-Dnlk-Exceed-Action (or SN1-Tp-Dnlk-Exceed-Action)	Specifies the downlink exceed action to perform.
SN-Tp-Dnlk-Violate-Action (or SN1-Tp-Dnlk-Violate-Action)	Specifies the downlink violate action to perform.
SN-QoS-Tp-Upk (or SN1-QoS-Tp-Upk)	Enable/disable traffic policing in the downlink direction.

Attribute	Description
SN-Tp-Uplk-Committed-Data-Rate (or SN1-Tp-Uplk-Committed-Data-Rate)	Specifies the uplink committed-data-rate in bps.
SN-Tp-Uplk-Peak-Data-Rate (or SN1-Tp-Uplk-Committed-Data-Rate)	Specifies the uplink peak-data-rate in bps.
SN-Tp-Uplk-Burst-Size (or SN1-Tp-Uplk-Burst-Size)	Specifies the uplink-burst-size in bytes. <b>NOTE:</b> It is recommended that this parameter be configured to at least the greater of the following two values: 1) 3 times greater than packet MTU for the subscriber connection, OR 2) 3 seconds worth of token accumulation within the “bucket” for the configured peak-data-rate.
SN-Tp-Uplk-Exceed-Action (or SN1-Tp-Uplk-Exceed-Action)	Specifies the uplink exceed action to perform.
SN-Tp-Uplk-Violate-Action (or SN1-Tp-Uplk-Violate-Action)	Specifies the uplink violate action to perform.

## Traffic Policing for UMTS Subscribers

The RADIUS attributes listed in the following table are used to configure Traffic Policing for UMTS subscribers configured on remote RADIUS servers. More information on these attributes can be found in the *AAA Interface Administration and Reference*.

**Table 51. RADIUS Attributes Required for Traffic Policing Support for UMTS Subscribers**

Attribute	Description
SN-QoS-Conversation-Class (or SN1-QoS-Conversation-Class)	Specifies the QoS Conversation Traffic Class.
SN-QoS-Streaming-Class (or SN1-QoS-Streaming-Class)	Specifies the QoS Streaming Traffic Class.

## ■ RADIUS Attributes

Attribute	Description
SN-QoS-Interactive1-Class (or SN1-QoS-Interactive1-Class)	Specifies the QoS Interactive Traffic Class.
SN-QoS-Interactive2-Class (or SN1-QoS-Interactive2-Class)	Specifies the QoS Interactive2 Traffic Class.
SN-QoS-Interactive3-Class (or SN1-QoS-Interactive3-Class)	Specifies the QoS Interactive3 Traffic Class.
SN-QoS-Background-Class (or SN1-QoS-Background-Class)	Specifies the QoS Background Traffic Class.
SN-QoS-Traffic-Policy (or SN1-QoS-Traffic-Policy)	This compound attribute simplifies sending QoS values for Traffic Class (the above attributes), Direction, Burst-Size, Committed-Data-Rate, Peak-Data-Rate, Exceed-Action, and Violate-Action from the RADIUS server. This attribute can be sent multiple times for different traffic classes. If Class is set to 0, it applies across all traffic classes.