



## **Cisco ASR 5000 Series Packet Data Network Gateway 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-25557-02

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 Packet Data Network Gateway Administration Guide

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

# CONTENTS

---

<b>About this Guide .....</b>	<b>xiii</b>
Conventions Used .....	xiv
Contacting Customer Support .....	xvi
Additional Information .....	xvii
<b>PDN Gateway Overview.....</b>	<b>19</b>
Product Description .....	20
Platform Requirements.....	22
Licenses .....	22
Network Deployment(s) .....	23
PDN Gateway in the E-UTRAN/EPC Network.....	23
Supported Logical Network Interfaces (Reference Points).....	24
PDN Gateway Supporting eHRPD to E-UTRAN/EPC Connectivity .....	29
Supported Logical Network Interfaces (Reference Points).....	30
Features and Functionality - Base Software .....	35
3GPP R9 Volume Charging Over Gx.....	36
AAA Server Groups.....	36
ANSI T1.276 Compliance.....	36
APN Support .....	37
Assume Positive for Gy-based Quota Tracking .....	38
Bulk Statistics Support .....	38
Congestion Control.....	39
Default and Dedicated EPC Bearers.....	40
DHCP Support.....	40
Direct Tunnel Support .....	41
Domain Based Flow Definitions .....	42
DSCP Marking.....	42
Dynamic Policy Charging Control (Gx Reference Interface).....	42
Enhanced Charging Service (ECS).....	43
Content Analysis Support .....	45
Content Service Steering .....	46
Support for Multiple Detail Record Types .....	46
Diameter Credit Control Application .....	47
Accept TCP Connections from DCCA Server.....	47
Gy Interface Support .....	47
Gn/Gp Handoff Support .....	48
IMS Emergency Bearer Handling.....	49
IP Access Control Lists .....	49
IP Address Hold Timers .....	50
IPv6 Capabilities.....	50
Local Break-Out .....	51
Management System Overview .....	51
Mobile IP Registration Revocation .....	52
Multiple PDN Support.....	53
Non-Optimized e-HRPD to Native LTE (E-UTRAN) Mobility Handover .....	53
Online/Offline Charging .....	54

Online Charging .....	54
Offline Charging .....	55
Proxy Mobile IPv6 (S2a).....	56
QoS Bearer Management .....	56
RADIUS Support .....	57
Source IP Address Validation.....	58
Subscriber Level Trace.....	58
Threshold Crossing Alerts (TCA) Support.....	59
UE Time Zone Reporting.....	60
Virtual APN Support .....	60
Features and Functionality - Inline Service Support.....	61
Content Filtering .....	61
Integrated Adult Content Filter .....	61
ICAP Interface.....	62
Header Enrichment: Header Insertion and Encryption.....	62
Mobile Video Gateway.....	63
Network Address Translation (NAT).....	64
NAT64 Support .....	64
Peer-to-Peer Detection.....	65
Personal Stateful Firewall.....	65
Traffic Performance Optimization (TPO).....	66
Features and Functionality - External Application Support .....	67
Web Element Management System.....	67
Features and Functionality - Optional Enhanced Feature Software.....	69
Always-On Licensing.....	69
GRE Protocol Interface Support.....	70
Inter-Chassis Session Recovery .....	70
IP Security (IPSec) Encryption .....	71
L2TP LAC Support .....	72
Lawful Intercept .....	72
Layer 2 Traffic Management (VLANs).....	72
Local Policy Decision Engine .....	73
MPLS Forwarding with LDP .....	73
NEMO Service Supported .....	74
Session Recovery Support.....	74
Smartphone Tethering Detection Support.....	74
Traffic Policing and Shaping.....	75
Traffic Policing.....	75
Traffic Shaping .....	75
User Location Information Reporting.....	76
How the PDN Gateway Works.....	78
PMIPv6 PDN Gateway Call/Session Procedures in an eHRPD Network .....	78
Initial Attach with IPv6/IPv4 Access .....	78
PMIPv6 Lifetime Extension without Handover .....	80
PDN Connection Release Initiated by UE.....	81
PDN Connection Release Initiated by HSGW .....	82
PDN Connection Release Initiated by P-GW.....	84
GTP PDN Gateway Call/Session Procedures in an LTE-SAE Network .....	85
Subscriber-initiated Attach (initial) .....	85
Subscriber-initiated Detach.....	88
Supported Standards.....	90
Release 9 3GPP References .....	90
Release 8 3GPP References .....	91
3GPP2 References.....	92

IETF References .....	92
Object Management Group (OMG) Standards .....	93
<b>PDN Gateway Configuration .....</b>	<b>95</b>
Configuring the System as a Standalone eGTP P-GW .....	96
Information Required .....	96
Required Local Context Configuration Information .....	96
Required P-GW Context Configuration Information .....	97
Required PDN Context Configuration Information .....	98
Required AAA Context Configuration Information .....	99
How This Configuration Works .....	102
eGTP P-GW Configuration .....	104
Initial Configuration .....	105
P-GW Service Configuration .....	110
P-GW PDN Context Configuration .....	111
Active Charging Service Configuration .....	112
Policy Configuration .....	115
Verifying and Saving the Configuration .....	118
Configuring the System as a Standalone PMIP P-GW Supporting an eHRPD Network .....	119
Information Required .....	119
Required Local Context Configuration Information .....	119
Required P-GW Context Configuration Information .....	120
Required PDN Context Configuration Information .....	121
Required AAA Context Configuration Information .....	122
How This Configuration Works .....	125
P-MIP P-GW (eHRPD) Configuration .....	127
Initial Configuration .....	128
P-GW Service Configuration .....	132
P-GW PDN Context Configuration .....	133
Active Charging Service Configuration .....	134
AAA and Policy Configuration .....	136
Verifying and Saving the Configuration .....	139
Configuring Optional Features on the P-GW .....	140
Configuring ACL-based Node-to-Node IP Security on the S5 Interface .....	140
Creating and Configuring a Crypto Access Control List .....	140
Creating and Configuring an IPSec Transform Set .....	141
Creating and Configuring an IKEv2 Transform Set .....	141
Creating and Configuring a Crypto Map .....	142
Configuring APN as Emergency .....	143
Configuring Dynamic Node-to-Node IP Security on the S5 Interface .....	144
Creating and Configuring an IPSec Transform Set .....	144
Creating and Configuring an IKEv2 Transform Set .....	145
Creating and Configuring a Crypto Template .....	145
Binding the S5 IP Address to the Crypto Template .....	146
Configuring Local QoS Policy .....	147
Creating and Configuring a Local QoS Policy .....	147
Binding a Local QoS Policy .....	148
Verifying Local QoS Policy .....	149
Configuring X.509 Certificate-based Peer Authentication .....	149
<b>Network Mobility (NEMO) .....</b>	<b>151</b>
NEMO Overview .....	152
Use Cases .....	152
Features and Benefits .....	153
MIPv4-based NEMO Control Plane .....	153

NEMO MR Authorization .....	154
MIPv4 NEMO Protocol .....	154
GRE Encapsulation .....	154
Session Interactions .....	154
NEMO Session Timers .....	155
Enterprise-wide Route Limit Control .....	155
Forced Fragmentation .....	155
Redundancy/Reliability .....	155
LTE NEMO Call Flow .....	156
Engineering Rules .....	158
Supported Standards .....	158
NEMO Configuration .....	159
Sample Configuration .....	159
Create a VRF .....	160
Set Neighbors and Address Family .....	161
Redistribute Connected Routes .....	161
Configure and Enable NEMO in APN Profile .....	161
Create a NEMO HA .....	162
<b>Configuring Subscriber Session Tracing .....</b>	<b>163</b>
Introduction .....	164
Supported Functions .....	165
Supported Standards .....	167
Subscriber Session Trace Functional Description .....	168
Operation .....	168
Trace Session .....	168
Trace Recording Session .....	168
Network Element (NE) .....	168
Activation .....	168
Management Activation .....	169
Signaling Activation .....	169
Start Trigger .....	169
Deactivation .....	169
Stop Trigger .....	169
Data Collection and Reporting .....	169
Trace Depth .....	169
Trace Scope .....	170
Network Element Details .....	170
MME .....	170
S-GW .....	170
P-GW .....	171
Subscriber Session Trace Configuration .....	172
Enabling Subscriber Session Trace on EPC Network Element .....	172
Trace File Collection Configuration .....	173
Verifying Your Configuration .....	174
<b>Monitoring the Service .....</b>	<b>177</b>
Monitoring System Status and Performance .....	178
Clearing Statistics and Counters .....	181
<b>Direct Tunnel .....</b>	<b>183</b>
Direct Tunnel Feature Overview .....	184
Direct Tunnel Configuration .....	188
Configuring Direct Tunnel Support on the SGSN .....	188
Enabling Setup of GTP-U Direct Tunnels .....	189

Enabling Direct Tunnel per APN .....	189
Enabling Direct Tunnel per IMEI .....	190
Enabling Direct Tunnel to Specific RNCs .....	190
Verifying the SGSN Direct Tunnel Configuration .....	191
Configuring S12 Direct Tunnel Support on the S-GW .....	193
<b>GRE Protocol Interface.....</b>	<b>195</b>
Introduction .....	196
Supported Standards.....	198
Supported Networks and Platforms.....	199
Licenses.....	200
Services and Application on GRE Interface .....	201
How GRE Interface Support Works.....	202
Ingress Packet Processing on GRE Interface.....	202
Egress Packet Processing on GRE Interface .....	204
GRE Interface Configuration .....	205
Virtual Routing And Forwarding (VRF) Configuration .....	205
GRE Tunnel Interface Configuration .....	206
Enabling OSPF for VRF .....	207
Associating IP Pool and AAA Group with VRF .....	207
Associating APN with VRF .....	208
Static Route Configuration .....	208
Verifying Your Configuration.....	209
<b>Gx Interface Support .....</b>	<b>211</b>
Rel. 6 Gx Interface.....	212
Introduction.....	212
Supported Networks and Platforms .....	212
License Requirements .....	212
Supported Standards .....	213
How it Works .....	213
Configuring Rel. 6 Gx Interface .....	215
Configuring IMS Authorization Service at Context Level .....	216
Verifying IMS Authorization Service Configuration .....	217
Applying IMS Authorization Service to an APN .....	217
Verifying Subscriber Configuration .....	218
Rel. 7 Gx Interface.....	219
Introduction.....	219
Supported Networks and Platforms .....	221
License Requirements .....	221
Supported Standards .....	221
Terminology and Definitions.....	222
Policy Control .....	222
Charging Control.....	225
Policy and Charging Control (PCC) Rules.....	226
PCC Procedures over Gx Reference Point .....	227
Volume Reporting Over Gx.....	229
How Rel. 7 Gx Works .....	232
Configuring Rel. 7 Gx Interface.....	235
Configuring IMS Authorization Service at Context Level .....	235
Applying IMS Authorization Service to an APN .....	237
Configuring Volume Reporting over Gx .....	238
Gathering Statistics .....	239
Rel. 8 Gx Interface.....	241
HA/PDSN Rel. 8 Gx Interface Support.....	241

Introduction.....	241
Terminology and Definitions.....	243
How it Works .....	249
Configuring HA/PDSN Rel. 8 Gx Interface Support .....	251
Gathering Statistics .....	254
P-GW Rel. 8 Gx Interface Support .....	255
Introduction.....	255
Terminology and Definitions.....	255
Rel. 9 Gx Interface .....	260
P-GW Rel. 9 Gx Interface Support .....	260
Introduction.....	260
Terminology and Definitions.....	260
<b>Gy Interface Support .....</b>	<b>265</b>
Introduction .....	266
License Requirements.....	268
Supported Standards.....	268
Features and Terminology.....	269
Charging Scenarios .....	269
Session Charging with Reservation .....	269
Basic Operations .....	269
Re-authorization .....	270
Threshold based Re-authorization Triggers.....	270
Termination Action .....	270
Diameter Base Protocol.....	270
Diameter Credit Control Application .....	271
Quota Behavior .....	272
Supported AVPs.....	284
Unsupported AVPs.....	288
Configuring Gy Interface Support .....	294
Configuring GGSN / P-GW / IPSP Gy Interface Support.....	294
Configuring HA / PDSN Gy Interface Support.....	295
Gathering Statistics .....	297
<b>ICAP Interface Support.....</b>	<b>299</b>
ICAP Interface Support Overview.....	300
Failure Action on Retransmitted Packets .....	301
Supported Networks and Platforms.....	302
License Requirements.....	302
Configuring ICAP Interface Support .....	303
Creating ICAP Server Group and Address Binding .....	303
Configuring ICAP Server and Other Parameters .....	304
Configuring ECS Rulebase for ICAP Server Group .....	304
Configuring Charging Action for ICAP Server Group .....	305
Verifying the ICAP Server Group Configuration .....	305
<b>IP Security.....</b>	<b>307</b>
Overview .....	309
Applicable Products and Relevant Sections .....	310
IPSec Terminology .....	313
Crypto Access Control List (ACL).....	313
Transform Set.....	313
ISAKMP Policy .....	313
Crypto Map .....	313
Manual Crypto Maps .....	314

ISAKMP Crypto Maps .....	314
Dynamic Crypto Maps .....	314
Implementing IPsec for PDN Access Applications .....	315
How the IPsec-based PDN Access Configuration Works .....	315
Configuring IPsec Support for PDN Access .....	316
Implementing IPsec for Mobile IP Applications.....	318
How the IPsec-based Mobile IP Configuration Works.....	318
Configuring IPsec Support for Mobile IP .....	321
Implementing IPsec for L2TP Applications .....	323
How IPsec is Used for Attribute-based L2TP Configurations.....	323
Configuring Support for L2TP Attribute-based Tunneling with IPsec.....	325
How IPsec is Used for PDSN Compulsory L2TP Configurations .....	326
Configuring Support for L2TP PDSN Compulsory Tunneling with IPsec .....	327
How IPsec is Used for L2TP Configurations on the GGSN.....	328
Configuring GGSN Support for L2TP Tunneling with IPsec.....	329
Transform Set Configuration .....	330
Configuring Transform Set .....	330
Verifying the Crypto Transform Set Configuration .....	330
ISAKMP Policy Configuration .....	332
Configuring ISAKMP Policy.....	332
Verifying the ISAKMP Policy Configuration .....	333
ISAKMP Crypto Map Configuration .....	334
Configuring ISAKMP Crypto Maps.....	334
Verifying the ISAKMP Crypto Map Configuration .....	335
Dynamic Crypto Map Configuration .....	337
Configuring Dynamic Crypto Maps .....	337
Verifying the Dynamic Crypto Map Configuration .....	337
Manual Crypto Map Configuration.....	339
Configuring Manual Crypto Maps.....	339
Verifying the Manual Crypto Map Configuration .....	340
Crypto Map and Interface Association .....	342
Applying Crypto Map to an Interface.....	342
Verifying the Interface Configuration with Crypto Map.....	342
FA Services Configuration to Support IPsec .....	344
Modifying FA service to Support IPsec.....	344
Verifying the FA Service Configuration with IPsec .....	345
HA Service Configuration to Support IPsec.....	346
Modifying HA service to Support IPsec .....	346
Verifying the HA Service Configuration with IPsec.....	347
RADIUS Attributes for IPsec-based Mobile IP Applications .....	348
LAC Service Configuration to Support IPsec.....	349
Modifying LAC service to Support IPsec .....	349
Verifying the LAC Service Configuration with IPsec.....	350
Subscriber Attributes for L2TP Application IPsec Support .....	351
PDSN Service Configuration for L2TP Support.....	352
Modifying PDSN service to Support Attribute-based L2TP Tunneling.....	352
Modifying PDSN service to Support Compulsory L2TP Tunneling .....	353
Verifying the PDSN Service Configuration for L2TP .....	353
Redundant IPsec Tunnel Fail-Over .....	354
Supported Standards .....	354
Redundant IPsec Tunnel Fail-over Configuration.....	355
Configuring Crypto Group .....	355
Modify ISAKMP Crypto Map Configuration to Match Crypto Group .....	356
Verifying the Crypto Group Configuration .....	356

Dead Peer Detection (DPD) Configuration .....	358
Configuring Crypto Group .....	358
Verifying the DPD Configuration .....	359
APN Template Configuration to Support L2TP .....	360
Modifying APN Template to Support L2TP .....	360
Verifying the APN Configuration for L2TP .....	361
IPSec for LTE/SAE Networks .....	362
Encryption Algorithms .....	362
HMAC Functions .....	362
Diffie-Hellman Groups .....	362
Dynamic Node-to-Node IPSec Tunnels .....	363
ACL-based Node-to-Node IPSec Tunnels .....	363
Traffic Selectors .....	363
Authentication Methods .....	364
X.509 Certificate-based Peer Authentication .....	364
Certificate Revocation Lists .....	366
Child SA Rekey Support .....	366
IKEv2 Keep-Alive Messages (Dead Peer Detection) .....	366
E-UTRAN/EPC Logical Network Interfaces Supporting IPSec Tunnels .....	367
IPSec Tunnel Termination .....	368
<b>L2TP Access Concentrator .....</b>	<b>369</b>
Applicable Products and Relevant Sections .....	370
Supported LAC Service Configurations for PDSN Simple IP .....	371
Attribute-based Tunneling .....	371
How The Attribute-based L2TP Configuration Works .....	372
Configuring Attribute-based L2TP Support for PDSN Simple IP .....	372
PDSN Service-based Compulsory Tunneling .....	373
How PDSN Service-based Compulsory Tunneling Works .....	373
Configuring L2TP Compulsory Tunneling Support for PDSN Simple IP .....	374
Supported LAC Service Configurations for the GGSN and P-GW .....	376
Transparent IP PDP Context Processing with L2TP Support .....	377
Non-transparent IP PDP Context Processing with L2TP Support .....	378
PPP PDP Context Processing with L2TP Support .....	379
Configuring the GGSN or P-GW to Support L2TP .....	380
Supported LAC Service Configuration for Mobile IP .....	381
How The Attribute-based L2TP Configuration for MIP Works .....	381
Configuring Attribute-based L2TP Support for HA Mobile IP .....	382
Configuring Subscriber Profiles for L2TP Support .....	384
RADIUS and Subscriber Profile Attributes Used .....	384
RADIUS Tagging Support .....	385
Configuring Local Subscriber Profiles for L2TP Support .....	385
Configuring Local Subscriber .....	386
Verifying the L2TP Configuration .....	386
Tunneling All Subscribers in a Specific Context Without Using RADIUS Attributes .....	387
Configuring LAC Services .....	388
Configuring LAC Service .....	388
Configuring LNS Peer .....	389
Verifying the LAC Service Configuration .....	389
Modifying PDSN Services for L2TP Support .....	391
Modifying PDSN Service .....	391
Verifying the PDSN Service for L2TP Support .....	392
Modifying APN Templates to Support L2TP .....	393
Assigning LNS Peer Address in APN Template .....	393
Configuring Outbound Authentication .....	394

Verifying the APN Configuration .....	394
<b>Mobile IP Registration Revocation.....</b>	<b>395</b>
Overview.....	396
Configuring Registration Revocation.....	398
Configuring FA Services .....	398
Configuring HA Services .....	398
<b>Proxy-Mobile IP .....</b>	<b>401</b>
Overview.....	402
Proxy Mobile IP in 3GPP2 Service.....	403
Proxy Mobile IP in 3GPP Service.....	403
Proxy Mobile IP in WiMAX Service .....	404
How Proxy Mobile IP Works in 3GPP2 Network .....	405
Scenario 1: AAA server and PDSN/FA Allocate IP Address.....	405
Scenario 2: HA Allocates IP Address.....	407
How Proxy Mobile IP Works in 3GPP Network .....	410
How Proxy Mobile IP Works in WiMAX Network.....	414
Scenario 1: AAA server and ASN GW/FA Allocate IP Address .....	414
Scenario 2: HA Allocates IP Address.....	416
How Proxy Mobile IP Works in a WiFi Network with Multiple Authentication.....	419
Configuring Proxy Mobile-IP Support.....	424
Configuring FA Services .....	424
Verify the FA Service Configuration .....	425
Configuring Proxy MIP HA Failover .....	425
Configuring HA Services .....	426
Configuring Subscriber Profile RADIUS Attributes .....	427
RADIUS Attributes Required for Proxy Mobile IP .....	427
Configuring Local Subscriber Profiles for Proxy-MIP on a PDSN .....	428
Configuring Local Subscriber Profiles for Proxy-MIP on a PDIF .....	429
Configuring Default Subscriber Parameters in Home Agent Context.....	429
Configuring APN Parameters.....	429
<b>Traffic Policing and Shaping .....</b>	<b>433</b>
Overview.....	434
Traffic Policing.....	434
Traffic Shaping .....	434
Traffic Policing Configuration.....	435
Configuring Subscribers for Traffic Policing .....	435
Configuring APN for Traffic Policing in 3GPP Networks .....	436
Traffic Shaping Configuration.....	438
Configuring Subscribers for Traffic Shaping .....	438
Configuring APN for Traffic Shaping in 3GPP Networks .....	439
RADIUS Attributes.....	442
Traffic Policing for CDMA Subscribers.....	442
Traffic Policing for UMTS Subscribers .....	443
<b>Sample Configuration Files .....</b>	<b>445</b>
Standalone eGTP PDN Gateway .....	446
Configuration Sample.....	446
Standalone PMIPv6 PDN Gateway Supporting an eHRPD Network.....	458
Configuration Sample.....	458
<b>P-GW Engineering Rules.....</b>	<b>469</b>
Interface and Port Rules.....	470
S2a Interface Rules.....	470

LMA to MAG.....	470
P-GW Context and Service Rules .....	471
P-GW Subscriber Rules.....	472

# 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: Login:
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

## PDN Gateway Overview

---

The Cisco® ASR 5x00 provides wireless carriers with a flexible solution that functions as Packet Data Network (PDN) Gateway (P-GW) in 3GPP2 Long Term Evolution-System Architecture Evolution (LTE-SAE) and evolved High Rate Packet Data (eHRPD) wireless data networks.

This overview provides general information about the P-GW including:

- [Product Description](#)
- [Network Deployment\(s\)](#)
- [Features and Functionality - Base Software](#)
- [Features and Functionality - Inline Service Support](#)
- [Features and Functionality - External Application Support](#)
- [Features and Functionality - Optional Enhanced Feature Software](#)
- [How the PDN Gateway Works](#)
- [Supported Standards](#)

# Product Description

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

Figure 1. P-GW in the Basic E-UTRAN/EPC Network

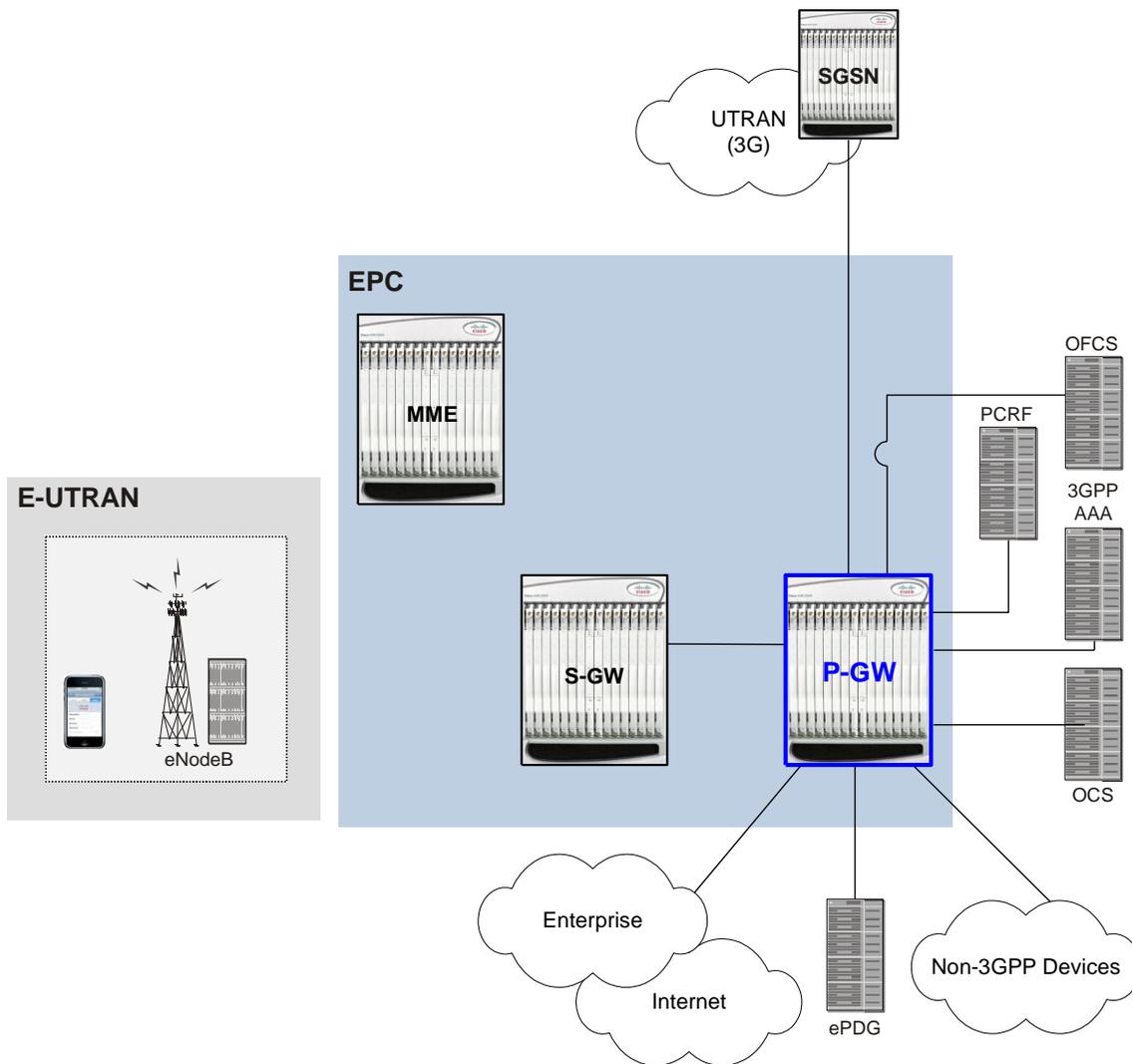
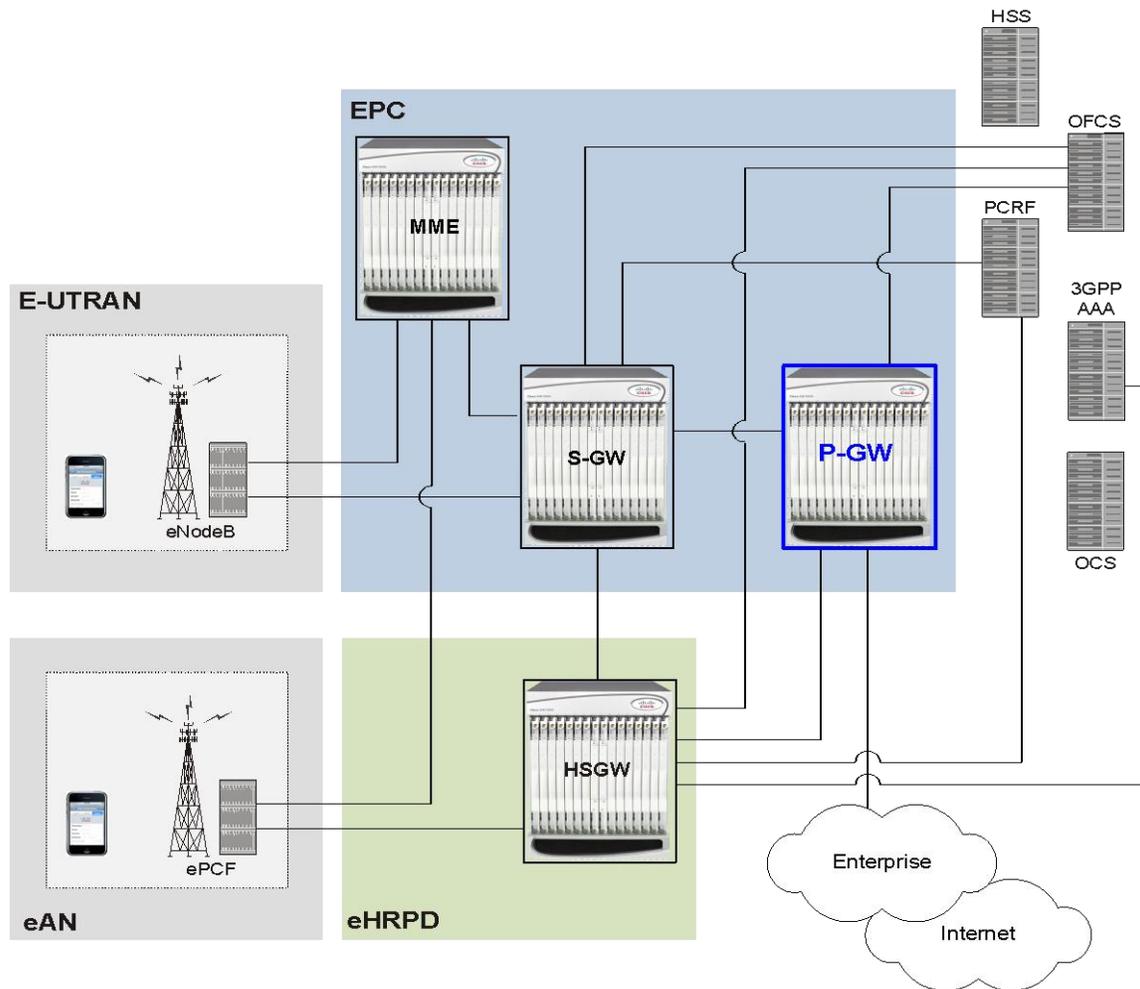


Figure 2. P-GW in the Basic E-UTRAN/EPC and eHRPD Network



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

P-GW functions include:

- Mobility anchor for mobility between 3GPP access systems and non-3GPP access systems. This is sometimes referred to as the SAE Anchor function.
- Policy enforcement (gating and rate enforcement)
- Per-user based packet filtering (deep packet inspection)
- Charging support
- Lawful Interception
- UE IP address allocation
- Packet screening
- Transport level packet marking in the downlink;
- Down link rate enforcement based on Aggregate Maximum Bit Rate (AMBR)

The following are additional P-GW functions when supporting non-3GPP access (eHRPD):

- P-GW includes the function of a Local Mobility Anchor (LMA) according to draft-ietf-netlmm-proxymip6, if PMIP-based S5 or S8 is used.
- The P-GW includes the function of a DSMIPv6 Home Agent, as described in draft-ietf-mip6-nemo-v4traversal, if S2c is used.

## Platform Requirements

The P-GW service runs on a Cisco® ASR 5x00 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.

## Licenses

The P-GW 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*.

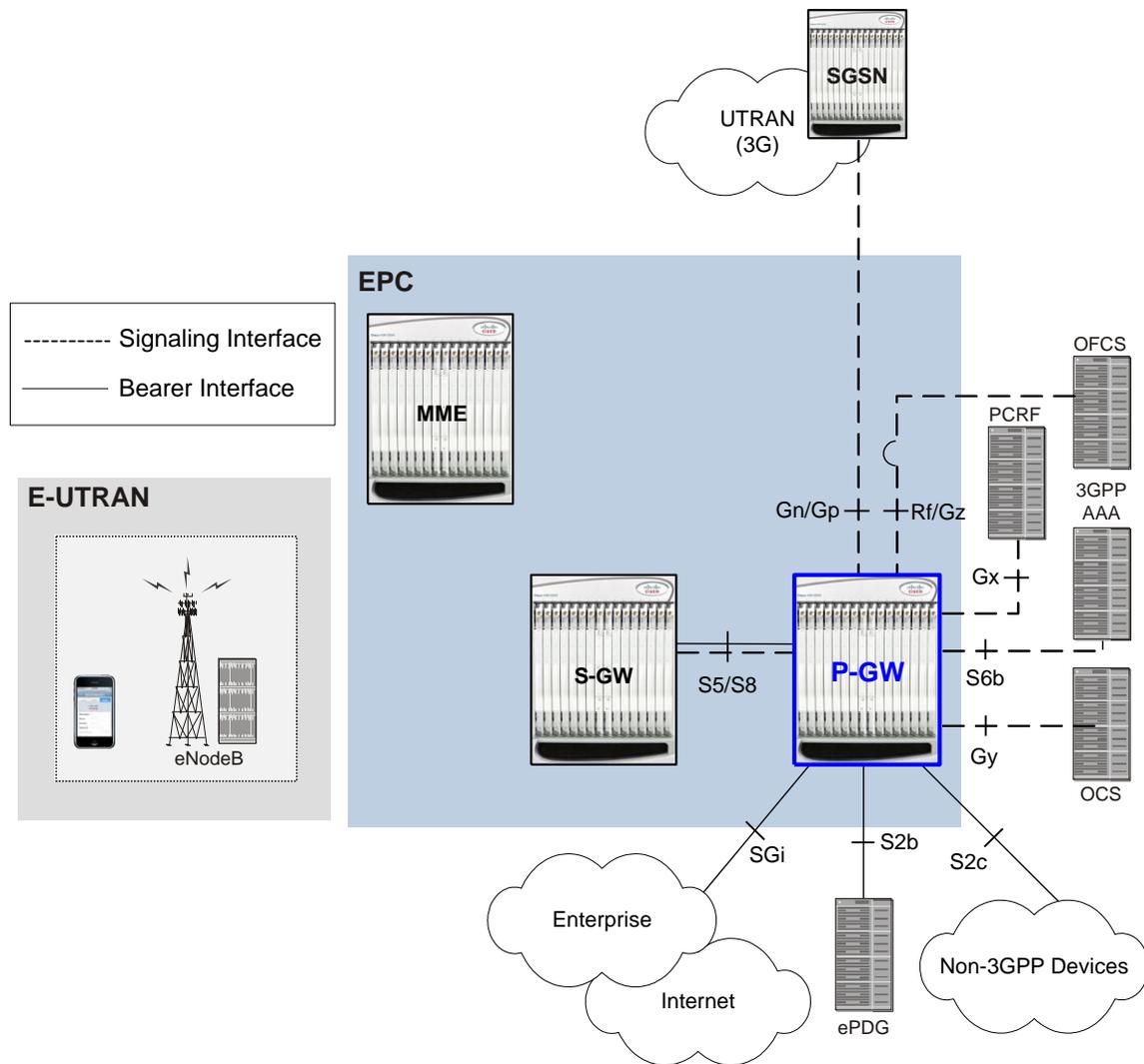
# Network Deployment(s)

This section describes the supported interfaces and the deployment scenarios of a PDN Gateway.

## PDN Gateway in the E-UTRAN/EPC Network

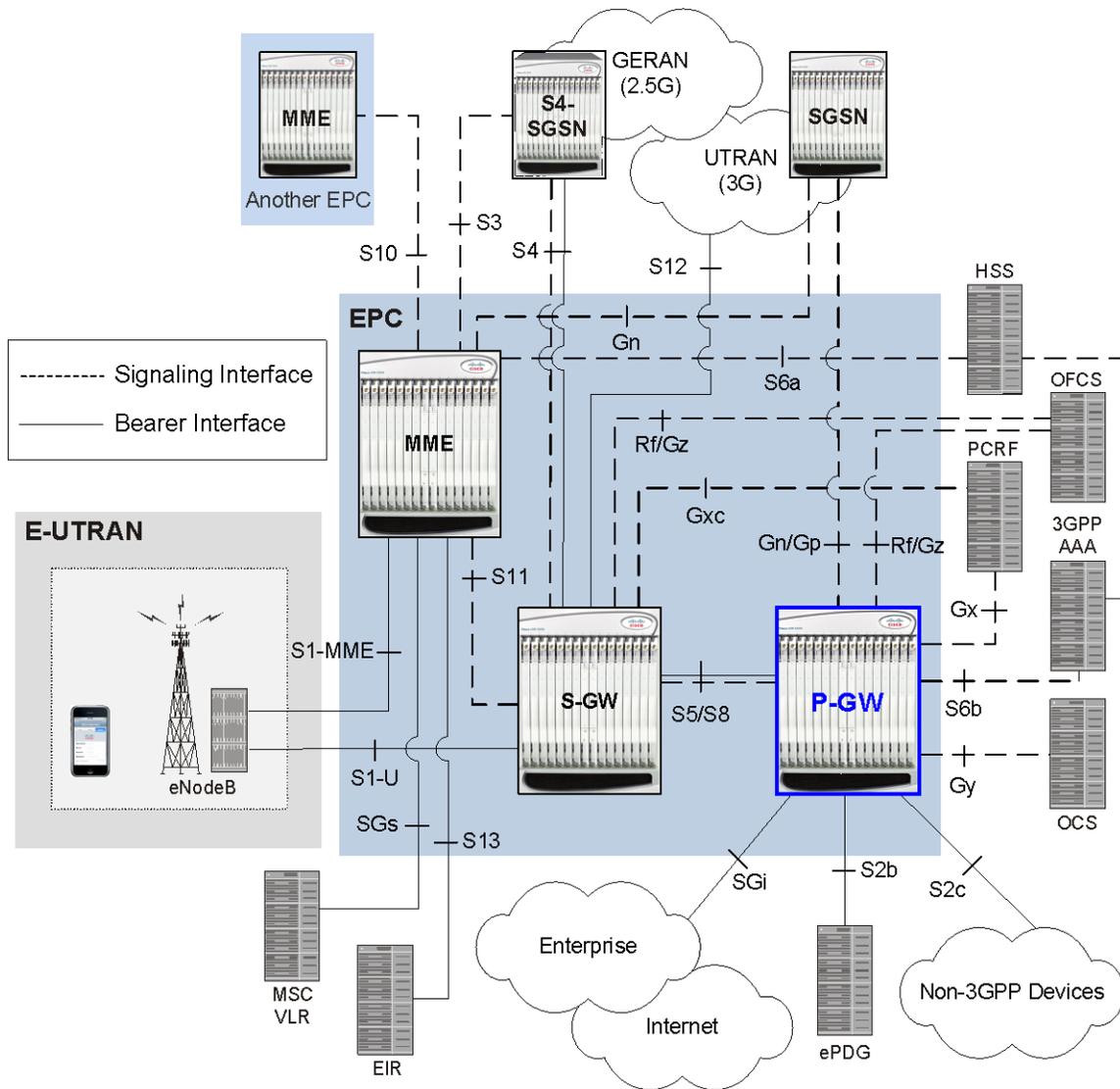
The following figure displays the specific network interfaces supported by the P-GW. Refer to [Supported Logical Network Interfaces \(Reference Points\)](#) for detailed information about each interface.

Figure 3. Supported P-GW Interfaces in the E-UTRAN/EPC Network



The following figure displays a sample network deployment of a P-GW, including all of the interface connections with other 3GPP Evolved-UTRAN/Evolved Packet Core network devices.

Figure 4. P-GW in the E-UTRAN/EPC Network



### Supported Logical Network Interfaces (Reference Points)

The P-GW provides the following logical network interfaces in support of E-UTRAN/EPC network:

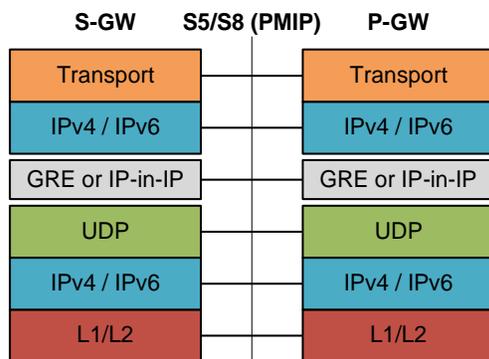
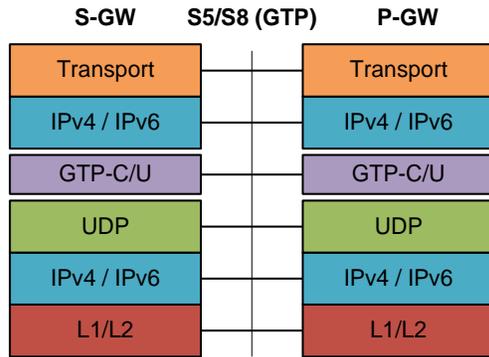
#### S5/S8 Interface

This reference point provides tunneling and management between the S-GW and the P-GW, as defined in 3GPP TS 23.401 and TS 23.402. The S8 interface is an inter-PLMN reference point between the S-GW and the P-GW used during roaming scenarios. The S5 interface is used between an S-GW and P-GW located within the same administrative domain (non-roaming). It is used for S-GW relocation due to UE mobility and if the S-GW needs to connect to a non-collocated P-GW for the required PDN connectivity.

#### Supported protocols

- Transport Layer: UDP, TCP

- Tunneling:
  - GTP: GTPv2-C (signaling channel), GTPv1-U (bearer channel)
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet



## S6b Interface

This reference point, between a P-GW and a 3GPP AAA server/proxy, is used for mobility-related authentication. It may also be used to retrieve and request parameters related to mobility and to retrieve static QoS profiles for UEs (for non-3GPP access) in the event that dynamic PCC is not supported.

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 CLI.

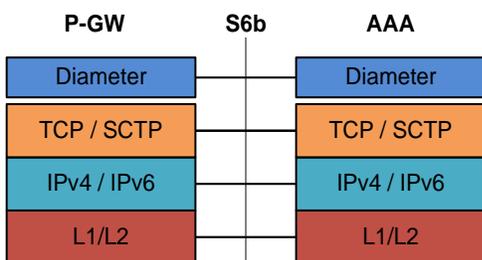
Another enhancement on S6b interface support is the new S6b retry-and-continue functionality that creates an automatic trigger in the GGSN and P-GW to use the locally configured APN profile upon receipt of any uniquely defined

Diameter error code on the S6b interface for an Authorization-Authentication-Request (AA-R) 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. In case of retry-and-continue functionality, P-GW should query from DNS server if it is configured in APN. S6b failure handling continues the data call. This behavior is only applicable to the aaa-custom15 Diameter dictionary.

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

**Supported protocols:**

- Transport Layer: TCP, SCTP
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet

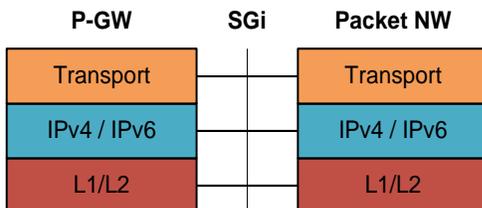


**SGi Interface**

This reference point provides connectivity between the P-GW and a packet data network (3GPP TS 23.401). This interface can provide access to a variety of network types including an external public or private PDN and/or an internal IMS service provisioning network.

**Supported protocols:**

- Transport Layer: TCP, UDP
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet

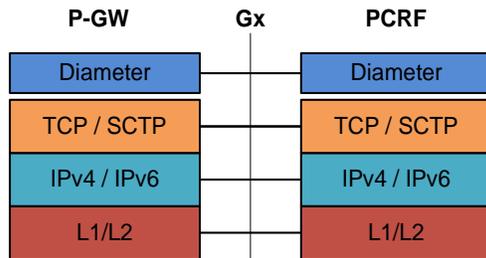


**Gx Interface**

This signalling interface supports the transfer of policy control and charging rules information (QoS) between the Policy and Charging Enforcement Function (PCEF) on the P-GW and a Policy and Charging Rules Function (PCRF) server (3GPP TS 23.401).

**Supported protocols:**

- Transport Layer: TCP, SCTP
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet



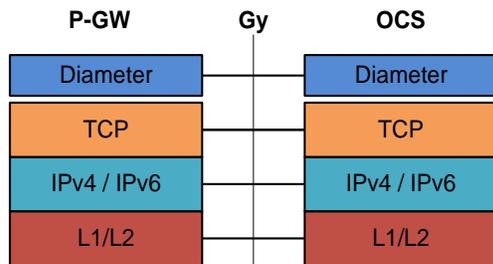
For more information on the Gx interface, refer to [Dynamic Policy Charging Control \(Gx Reference Interface\)](#) in the *Features and Functionality - Base Software* section of this chapter.

## Gy Interface

The Gy reference interface enables online accounting functions on the P-GW in accordance with 3GPP Release 8 and Release 9 specifications.

### Supported protocols:

- Transport Layer: TCP
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet



For more information on the Gy interface and online accounting, refer to [Gy Interface Support](#) in the *Features and Functionality - Base Software* section of this chapter.

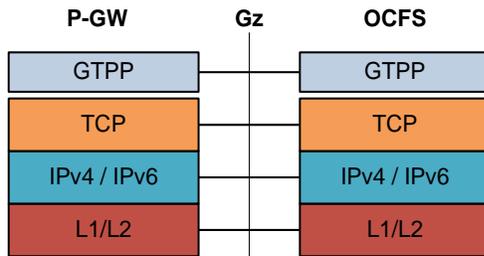
## Gz Interface

The Gz reference interface enables offline accounting functions on the P-GW. The P-GW collects charging information for each mobile subscriber UE pertaining to the radio network usage.

### Supported protocols:

- Transport Layer: TCP
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP

- Physical Layer: Ethernet

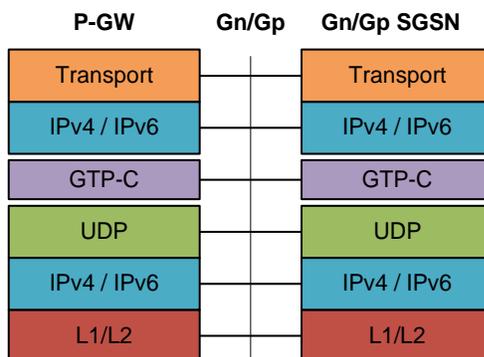


## Gn/Gp Interface

This reference point provides tunneling and management between the P-GW and the SGSN during handovers between the EPS and 3GPP 2G and/or 3G networks (3GPP TS 29.060). For more information on the Gn/Gp interface, refer to [Gn/Gp Handoff Support](#) in the *Features and Functionality - Base Software* section of this chapter.

### Supported protocols

- Transport Layer: UDP, TCP
- Tunneling: GTP: GTP-C (signaling channel)
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet

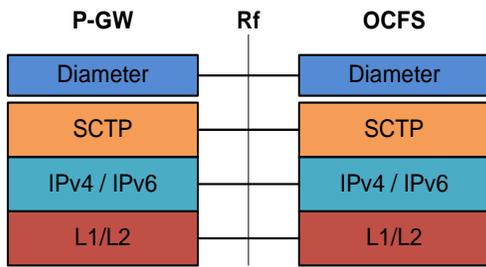


## Rf Interface

The Rf interface enables offline accounting functions on the P-GW in accordance with 3GPP Release 8 and Release 9 specifications. The P-GW collects charging information for each mobile subscriber UE pertaining to the radio network usage.

### Supported protocols:

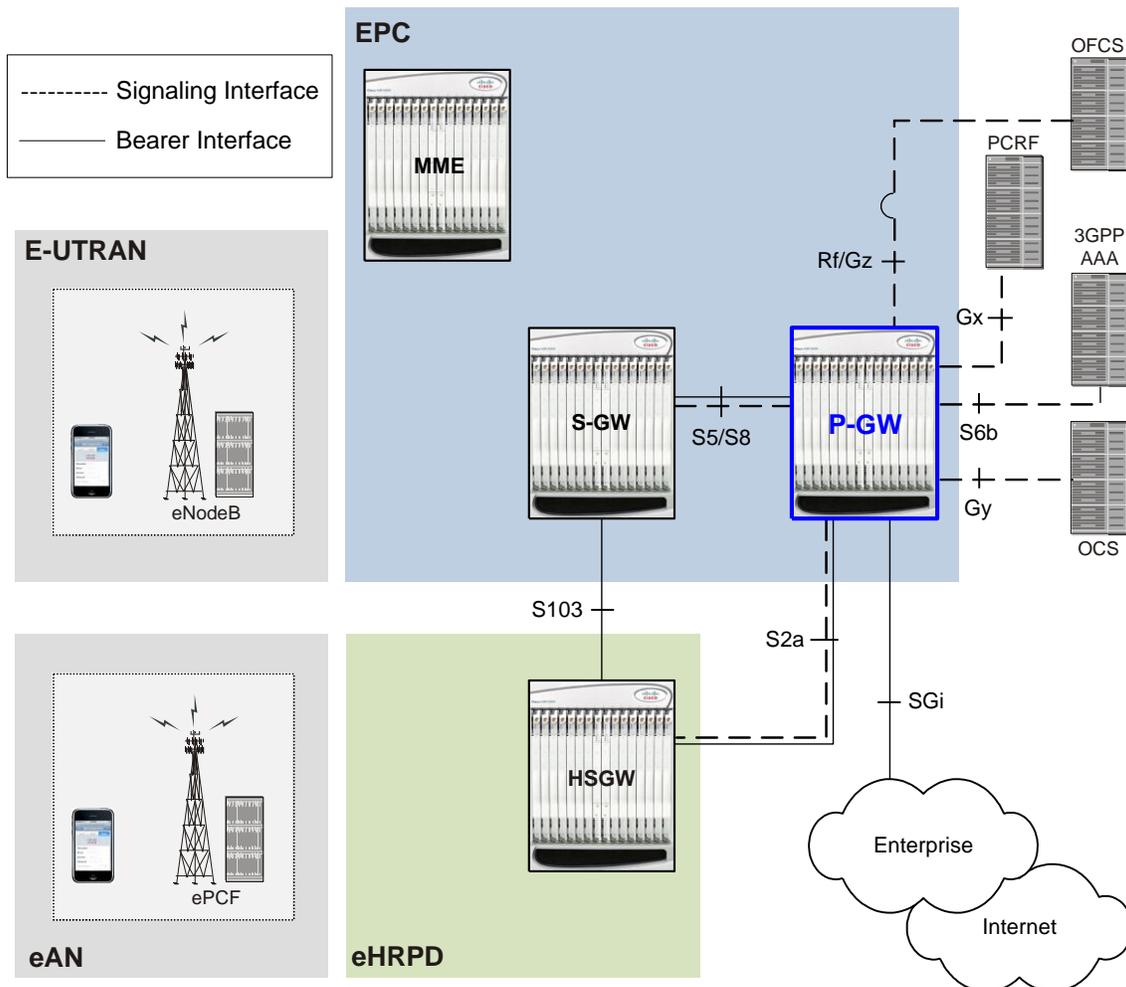
- Transport Layer: TCP
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet



## PDN Gateway Supporting eHRPD to E-UTRAN/EPC Connectivity

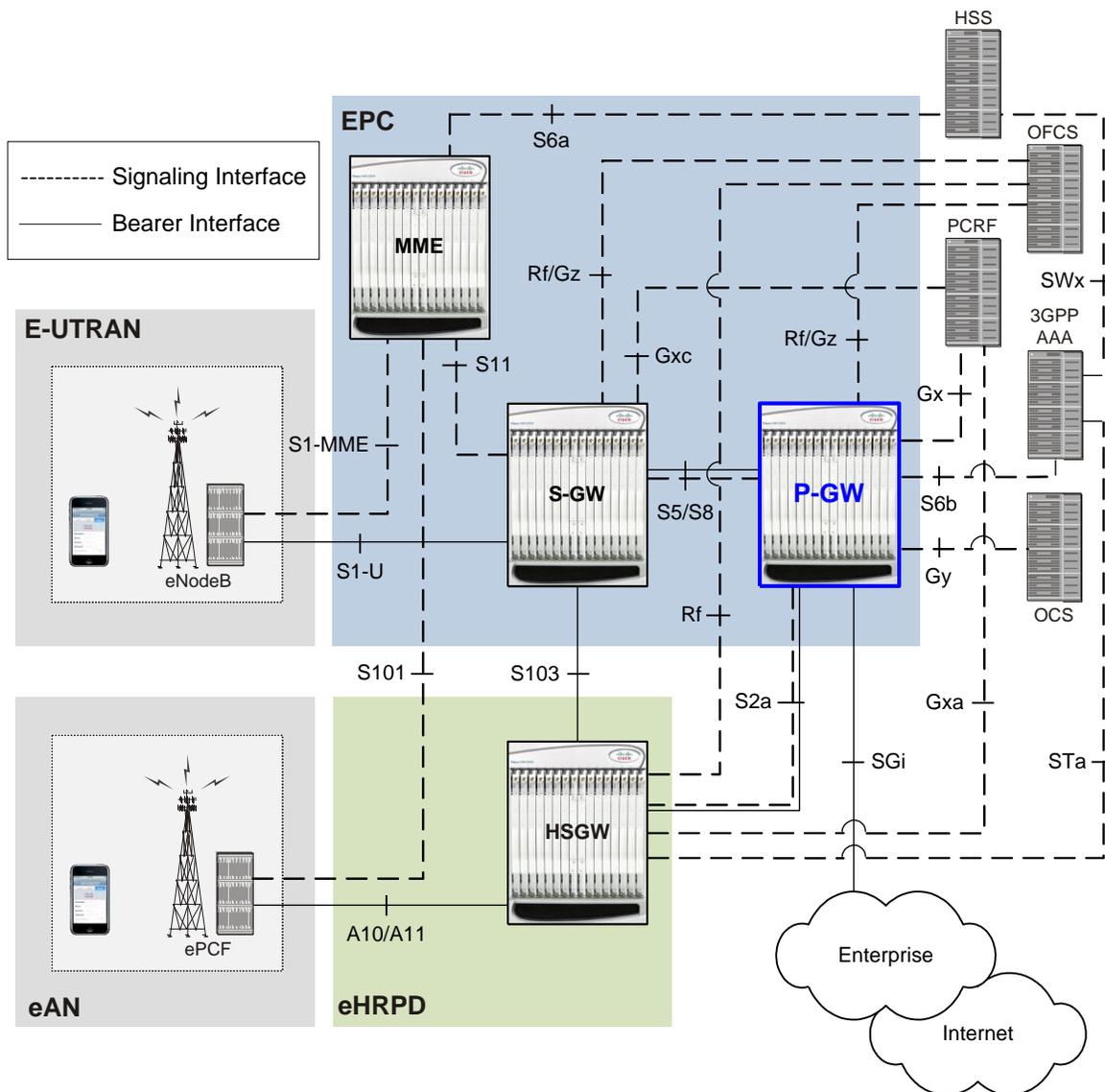
The following figure displays the specific network interfaces supported by the P-GW in an eHRPD network. Refer to [Supported Logical Network Interfaces \(Reference Points\)](#) for detailed information about each interface.

Figure 5. P-GW Interfaces Supporting eHRPD to E-UTRAN/EPC Connectivity



The following figure displays a sample network deployment of a P-GW in an eHRPD Network, including all of the interface connections with other 3GPP Evolved-UTRAN/Evolved Packet Core network devices.

Figure 6. P-GW in the E-UTRAN/EPC Network Supporting the eHRPD Network



## Supported Logical Network Interfaces (Reference Points)

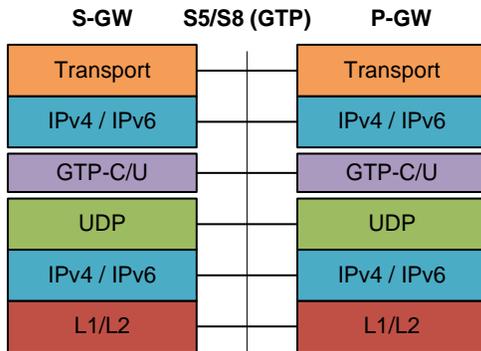
The P-GW provides the following logical network interfaces in support of eHRPD to E-UTRAN/EPC connectivity:

### S5/S8 Interface

This reference point provides tunneling and management between the S-GW and the P-GW, as defined in 3GPP TS 23.401. The S8 interface is an inter-PLMN reference point between the S-GW and the P-GW used during roaming scenarios. The S5 interface is used between an S-GW and P-GW located within the same administrative domain (non-roaming). It is used for S-GW relocation due to UE mobility and if the S-GW needs to connect to a non-collocated P-GW for the required PDN connectivity.

**Supported protocols:**

- Transport Layer: UDP, TCP
- Tunneling:
  - GTP: IPv4 or IPv6 GTP-C (signaling channel) and GTP-U (bearer channel)
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet

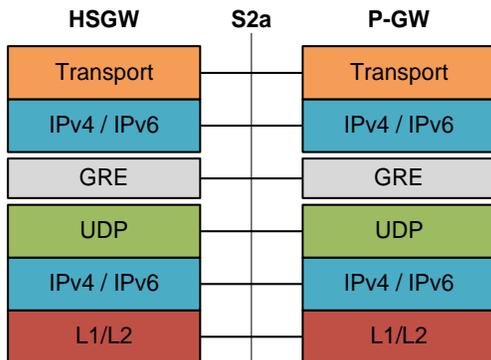


### S2a Interface

This reference point supports the bearer interface by providing signaling and mobility support between a trusted non-3GPP access point (HSGW) and the PDN Gateway. It is based on Proxy Mobile IP but also supports Client Mobile IPv4 FA mode which allows connectivity to trusted non-3GPP IP access points that do not support PMIP.

**Supported protocols:**

- Transport Layer: UDP, TCP
- Tunneling: GRE IPv6
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet



### S6b Interface

This reference point, between a P-GW and a 3GPP AAA server/proxy, is used for mobility-related authentication. It may also be used to retrieve and request parameters related to mobility and to retrieve static QoS profiles for UEs (for non-3GPP access) in the event that dynamic PCC is not supported.

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 CLI.

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 (AA-R) 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. In case of retry-and-continue functionality, P-GW should query from DNS server if it is configured in APN. S6b failure handling continues the data call. This behavior is only applicable to the aaa-custom15 Diameter dictionary.

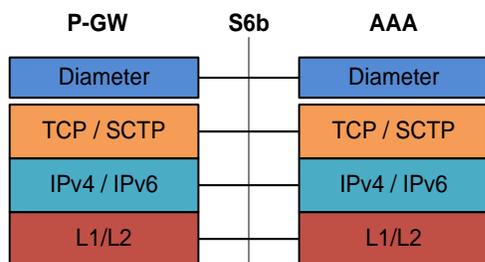
---

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

---

**Supported protocols:**

- Transport Layer: TCP, SCTP
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet

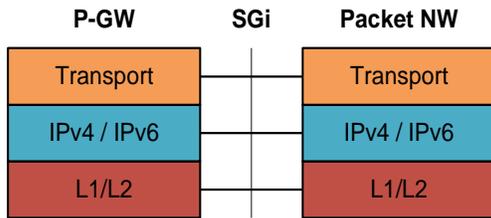


**SGi Interface**

This reference point provides connectivity between the P-GW and a packet data network. This interface can provide access to a variety of network types including an external public or private PDN and/or an internal IMS service provisioning network.

**Supported protocols:**

- Transport Layer: TCP, UDP
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet

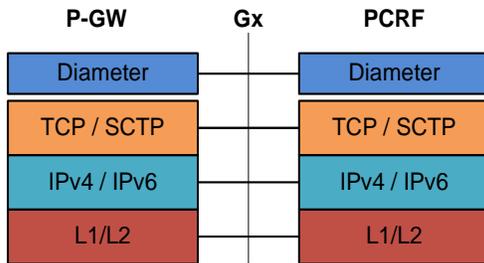


## Gx Interface

This signalling interface supports the transfer of policy control and charging rules information (QoS) between the Policy and Charging Enforcement Function (PCEF) on the P-GW and a Policy and Charging Rules Function (PCRF) server (3GPP TS 23.401).

### Supported protocols:

- Transport Layer: TCP, SCTP
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet



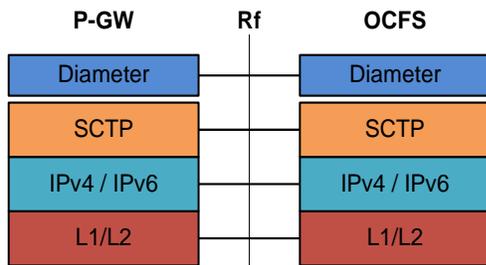
For more information on the Gx interface, refer to [Dynamic Policy Charging Control \(Gx Reference Interface\)](#) in the *Features and Functionality - Base Software* section of this chapter.

## Rf Interface

The Rf reference interface enables offline accounting functions on the P-GW in accordance with 3GPP Release 8 and Release 9 specifications. The P-GW collects charging information for each mobile subscriber UE pertaining to the radio network usage.

### Supported protocols:

- Transport Layer: TCP
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet



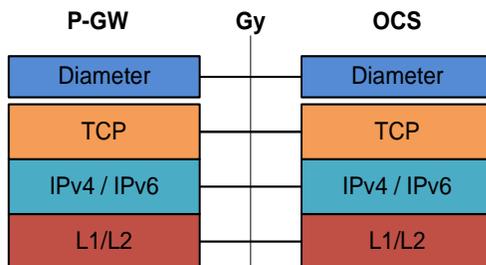
For more information on Rf accounting, refer to the section in the *Features and Functionality - Base Software* section of this chapter.

## Gy Interface

The Gy reference interface enables online accounting functions on the P-GW in accordance with 3GPP Release 8 and Release 9 specifications.

### Supported protocols:

- Transport Layer: TCP
- Network Layer: IPv4, IPv6
- Data Link Layer: ARP
- Physical Layer: Ethernet



For more information on the Gy interface and online accounting, refer to [Gy Interface Support](#) in the *Features and Functionality - Base Software* section of this chapter.

## Features and Functionality - Base Software

This section describes the features and functions supported by default in the base software for the P-GW service and do not require any additional licenses to implement the functionality.

This section describes the following features:

- 3GPP R9 Volume Charging Over Gx
- AAA Server Groups
- ANSI T1.276 Compliance
- APN Support
- Assume Positive for Gy-based Quota Tracking
- Bulk Statistics Support
- Congestion Control
- Default and Dedicated EPC Bearers
- DHCP Support
- Direct Tunnel Support
- Domain Based Flow Definitions
- DSCP Marking
- Dynamic Policy Charging Control (Gx Reference Interface)
- Enhanced Charging Service (ECS)
- GnGp Handoff Support
- IMS Emergency Bearer Handling
- IP Access Control Lists
- IP Address Hold Timers
- IPv6 Capabilities
- Local Break-Out
- Management System Overview
- Mobile IP Registration Revocation
- Non-Optimized e-HRPD to Native LTE (E-UTRAN) Mobility Handover
- Multiple PDN Support
- Online/Offline Charging
- Proxy Mobile IPv6 (S2a)
- QoS Bearer Management
- RADIUS Support
- Source IP Address Validation
- Subscriber Level Trace
- Threshold Crossing Alerts (TCA) Support

- [UE Time Zone Reporting](#)
- [Virtual APN Support](#)



**Important:** To configure the basic service and functionality on the system for the P-GW service, refer to the configuration examples provided in this guide.

## 3GPP R9 Volume Charging Over Gx

Also known as accumulated usage tracking over Gx, this 3GPP R9 enhancement provides a subset of the volume and charging control functions defined in TS 29.212 based on usage quotas between a P-GW and PCRF. The quotas can be assigned to the default bearer or any of the dedicated bearers for the PDN connection.

This feature enables volume reporting over Gx, which entails usage monitoring and reporting of the accumulated usage of network resources on an IP-CAN session or service data flow basis. PCRF subscribes to the usage monitoring at session level or at flow level by providing the necessary information to PCEF. PCEF in turn reports the usage to the PCRF when the conditions are met. Based on the total network usage in real-time, the PCRF will have the information to enforce dynamic policy decisions.

When usage monitoring is enabled, the PCEF can monitor the usage volume for the IP-CAN session, or applicable service data flows, and report accumulated usage to the PCRF based on any of the following conditions:

- When a usage threshold is reached,
- When all PCC rules for which usage monitoring is enabled for a particular usage monitoring key are removed or deactivated,
- When usage monitoring is explicitly disabled by the PCRF,
- When an IP CAN session is terminated or,
- When requested by the PCRF.

Accumulated volume reporting can be measured by total volume, the uplink volume, or the downlink volume as requested by the PCRF. When receiving the reported usage from the PCEF, the PCRF deducts the value of the usage report from the total allowed usage for that IP-CAN session, usage monitoring key, or both as applicable.

## 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 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.

## 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 ASR 5x00 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 P-GW'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 P-GW. 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 P-GW, Mobile IP, DHCP, 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 P-GW 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 P-GW, the subscriber may be authenticated/authorized with an AAA server. The P-GW 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 P-GW during subscriber authentication/authorization.

---

 **Important:** For more information on APN configuration, refer to the *PDN Gateway Configuration* chapter in this guide.

---

## Assume Positive for Gy-based Quota Tracking

In the current implementation, the PCEF uses a Diameter based Gy interface to interact with the OCS and obtain quota for each subscriber's data session. Now, the PCEF can retry the OCS after a configured amount of quota has been utilized or after a configured amount of time. The quota value would be part of the dcca-service configuration, and would apply to all subscribers using this dcca-service. The temporary quota will be specified in volume (MB) and/or time (minutes) to allow for enforcement of both quota tracking mechanisms, individually or simultaneously.

When a user consumes the interim total quota or time configured for use during failure handling scenarios, the PCEF shall retry the OCS server to determine if functionality has been restored. In the event that services have been restored, quota assignment and tracking will proceed as per standard usage reporting procedures. Data used during the outage will be reported to the OCS. In the event that the OCS services have not been restored, the PCEF should reallocate with the configured amount of quota and time assigned to the user. The PCEF should report all accumulated used data back to OCS when OCS is back online. If multiple retries and interim allocations occur, the PCEF shall report quota used during all allocation intervals.

When the Gy interface is unavailable, the P-GW shall enter “assume positive” mode. Unique treatment is provided to each subscriber type. Each functional application shall be assigned unique temporary quota volume amounts and time periods based on a command-level AVP from the PCRF on the Gx interface. In addition, a configurable option has been added to disable assume positive functionality for a subscriber group identified by a command-level AVP sent on the Gx interface by the PCRF.

## 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.

Following is a list of supported schemas for P-GW:

- **APN:** Provides Access Point Name statistics
- **Card:** Provides card-level statistics
- **Context:** Provides context service statistics
- **Diameter-acct:** Provides Diameter Accounting statistics
- **Diameter-auth:** Provides Diameter Authentication statistics
- **ECS:** Provides Enhanced Charging Service statistics
- **EGTPC:** Provides Evolved GPRS Tunneling Protocol - Control message statistics
- **FA:** Provides FA service statistics
- **GTPC:** Provides GPRS Tunneling Protocol - Control message statistics
- **GTPP:** Provides GPRS Tunneling Protocol - Prime message statistics
- **GTPU:** Provides GPRS Tunneling Protocol - User message statistics
- **HA:** Provides HA service statistics
- **IMSA:** Provides IMS Authorization service statistics
- **IP Pool:** Provides IP pool statistics

- **LMA:** Provides Local Mobility Anchor service statistics
- **P-GW:** Provides P-GW node-level service statistics
- **Port:** Provides port-level statistics
- **PPP:** Provides Point-to-Point Protocol statistics
- **RADIUS:** Provides per-RADIUS server statistics
- **System:** Provides system-level 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.

---

 **Important:** For more information on bulk statistic configuration, refer to the *Configuring and Maintaining Bulk Statistics* chapter in the *System Administration Guide*.

---

## Congestion Control

The congestion control feature allows you to set policies and thresholds and specify how the system reacts when faced with a heavy load condition.

Congestion control monitors the system for conditions that could potentially degrade performance when the system is under heavy load. Typically, these conditions are temporary (for example, high CPU or memory utilization) and are quickly resolved. However, continuous or large numbers of these conditions within a specific time interval may have an impact the system's ability to service subscriber sessions. Congestion control helps identify such conditions and invokes policies for addressing the situation.

Congestion control operation is based on configuring the following:

- **Congestion Condition Thresholds:** Thresholds dictate the conditions for which congestion control is enabled and establishes limits for defining the state of the system (congested or clear). These thresholds function in a way similar to operation thresholds that are configured for the system as described in the Thresholding Configuration Guide. The primary difference is that when congestion thresholds are reached, a service congestion policy and an SNMP trap, `starCongestion`, are generated.

A threshold tolerance dictates the percentage under the configured threshold that must be reached in order for the condition to be cleared. An SNMP trap, `starCongestionClear`, is then triggered.

- **Port Utilization Thresholds:** If you set a port utilization threshold, when the average utilization of all ports in the system reaches the specified threshold, congestion control is enabled.
  - **Port-specific Thresholds:** If you set port-specific thresholds, when any individual port-specific threshold is reached, congestion control is enabled system-wide.
- **Service Congestion Policies:** Congestion policies are configurable for each service. These policies dictate how services respond when the system detects that a congestion condition threshold has been crossed.



**Important:** For more information on congestion control, refer to the *Congestion Control* chapter in the *System Administration Guide*.

## Default and Dedicated EPC Bearers

Provides a foundation for contributing towards improved Quality of User Experience (QoE) by enabling deterministic end-to-end forwarding and scheduling treatments for different services or classes of applications pursuant to their requirements for committed bandwidth resources, jitter and delay. In this way, each application receives the service treatment that users expect.

In the StarOS 9.0 release, the Cisco EPC core platforms support one or more EPS bearers (default plus dedicated). An EPS bearer is a logical aggregate of one or more Service Data Flows (SDFs), running between a UE and a P-GW in the case of a GTP-based S5/S8 interface, and between a UE and HSGW (HRPD Serving Gateway) in case of a PMIP-based S2a interface. In networks where GTP is used as the S5/S8 protocol, the EPS bearer constitutes a concatenation of a radio bearer, S1-U bearer and an S5/S8 bearer anchored on the P-GW. In cases where PMIPv6 is used the EPS bearer is concatenated between the UE and HSGW with IP connectivity between the HSGW and P-GW.

Note: This release supports only GTP-based S5/S8 and PMIPv6 S2a capabilities with no commercial support for PMIPv6 S5/S8.

An EPS bearer uniquely identifies traffic flows that receive a common QoS treatment between a UE and P-GW in the GTP-based S5/S8 design, and between a UE and HSGW in the PMIPv6 S2a approach. If different QoS scheduling priorities are required between Service Data Flows, they should be assigned to separate EPS bearers. Packet filters are signalled in the NAS procedures and associated with a unique packet filter identifier on a per-PDN connection basis.

One EPS bearer is established when the UE connects to a PDN, and that remains established throughout the lifetime of the PDN connection to provide the UE with always-on IP connectivity to that PDN. That bearer is referred to as the default bearer. A PDN connection represents a traffic flow aggregate between a mobile access terminal and an external Packet Data Network (PDN) such as an IMS network, a walled garden application cloud or a back-end enterprise network. Any additional EPS bearer that is established to the same PDN is referred to as a dedicated bearer. The EPS bearer Traffic Flow Template (TFT) is the set of all 5-tuple packet filters associated with a given EPS bearer. The EPC core elements assign a separate bearer ID for each established EPS bearer. At a given time a UE may have multiple PDN connections on one or more P-GWs.

## DHCP Support

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

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

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

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

The P-GW does not support DHCP-relay.

---

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

---

### Deferred IPv4 Address Allocation

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

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

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

## Direct Tunnel Support

When Gn/Gp interworking with pre-release SGSNs is enabled, the GGSN service on the P-GW supports direct tunnel functionality.

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 toward the GGSN).

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

---

 **Important:** For more information on direct tunnel support, refer to the *Direct Tunnel* appendix in this guide.

---

## Domain Based Flow Definitions

This solution provides improved flexibility and granularity in obtaining geographically correct exact IP entries of the servers by snooping DNS responses.

Currently, it is possible to configure L7 rules to filter based on domain (m.google.com). Sometimes multiple servers may serve a domain, each with its own IP address. Using an IP-rule instead of an http rule will result in multiple IP-rules; one IP-rule for each server “behind” the domain, and it might get cumbersome to maintain a list of IP addresses for domain-based filters.

In this solution, you can create ruledefs specifying hostnames (domain names) and parts of hostnames (domain names). Upon the definition of the hostnames/domain names or parts of them, the P-GW will monitor all the DNS responses sent towards the UE and will snoop only the DNS response, which has q-name or a-name as specified in the rules, and identify all the IP addresses resulted from the DNS responses. DNS snooping will be done on live traffic for every subscriber.

## DSCP Marking

Provides support for more granular configuration of DSCP marking.

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

The following matrix may be used to determine the Diffserv markings used based on the configured traffic class and Allocation/Retention Priority:

**Table 1. Default DSCP Value Matrix**

Allocation Priority	1	2	3
Traffic Handling Priority			
1	ef	ef	ef
2	af21	af21	af21
3	af21	af21	af21

In addition, the P-GW allows configuration of diameter packets with DSCP values.

## Dynamic Policy Charging Control (Gx Reference Interface)

Dynamic policy and charging control provides a primary building block toward the realization of IMS multimedia applications. In contrast to statically provisioned architectures, the dynamic policy framework provides a centralized service control layer with global awareness of all access-side network elements. The centralized policy decision elements simplify the process of provisioning global policies to multiple access gateways. Dynamic policy is especially useful in an Always-On deployment model as the usage paradigm transitions from a short lived to a lengthier online session in which the volume of data consumed can be extensive. Under these conditions dynamic policy management enables dynamic just in-time resource allocation to more efficiently protect the capacity and resources of the network.

Dynamic Policy Control represents the ability to dynamically authorize and control services and application flows between a Policy Charging Enforcement Function (PCEF) on the P-GW and the PCRF. Policy control enables a

centralized and decoupled service control architecture to regulate the way in which services are provisioned and allocated at the bearer resource layer.

The StarOS 9.0 release included enhancements to conform with 3GPP TS 29.212 and 29.230 functions. The Gx reference interface uses Diameter transport and IPv6 addressing. The subscriber is identified to the PCRF at session establishment using IMSI based NAI's within the Subscription-ID AVP. Additionally the IMEI within the Equipment-Info AVP is used to identify the subscriber access terminal to the policy server. The Gx reference interface supports the following capabilities:

- Authorize the bearer establishment for a packet flow
- Dynamic L3/L4 transfer of service data flow filters within PCC rules for selection and policy enforcement of downlink/uplink IP CAN bearers
- Support static pre-provisioned L7 rulebase name attribute as trigger for activating Inline Services such as Peer-to-Peer Detection
- Authorize the modification of a service data flow
- Revoke the authorization of a packet flow
- Provision PCC rules for service data flows mapped to default or dedicated EPS bearers
- Support P-GW initiated event triggers based on change of access network gateway or IP CAN
- Provide the ability to set or modify APN-AMBR for a default EPS bearer
- Create or modify QoS service priority by including QCI values in PCC rules transmitted from PCRF to PCEF functions

## Enhanced Charging Service (ECS)

The Enhanced Charging Service provides an integrated in-line service for inspecting subscriber data packets and generating detail records to enable billing based on usage and traffic patterns. Other features include:

- [Content Analysis Support](#)
- [Content Service Steering](#)
- [Support for Multiple Detail Record Types](#)
- [Diameter Credit Control Application](#)
- [Accept TCP Connections from DCCA Server](#)
- [Gy Interface Support](#)

The Enhanced Charging Service (ECS) is an in-line service feature that is integrated within the system. ECS enhances the mobile carrier's ability to provide flexible, differentiated, and detailed billing to subscribers by using Layer 3 through Layer 7 deep packet inspection with the ability to integrate with back-end billing mediation systems.

ECS interacts with active mediation systems to provide full real-time prepaid and active charging capabilities. Here the active mediation system provides the rating and charging function for different applications.

In addition, ECS also includes extensive record generation capabilities for post-paid charging with in-depth understanding of the user session. Refer to the Support for Multiple Detail Record Types section for more information.

The major components include:

- **Service Steering:** Directs subscriber traffic into the ECS subsystem. Service Steering is used to direct selective subscriber traffic flows via an Access Control List (ACL). It is used for other redirection applications as well for both internal and external services and servers.

- **Protocol Analyzer:** The software stack responsible for analyzing the individual protocol fields and states during packet inspection. It performs two types of packet inspection:
  - **Shallow Packet Inspection:** inspection of the layer 3 (IP header) and layer 4 (e.g. UDP or TCP header) information.
  - **Deep Packet Inspection:** inspection of layer 7 and 7+ information. Deep packet inspection functionality includes:
    - Detection of URI (Uniform Resource Identifier) information at level 7 (e.g., HTTP, WTP, RTSP Uniform Resource Locators (URLs)).
    - Identification of true destination in the case of terminating proxies, where shallow packet inspection would only reveal the destination IP address / port number of a terminating proxy.
    - De-encapsulation of upper layer protocol headers, such as MMS-over-WTP, WSP-over-UDP, and IP-over GPRS.
    - Verification that traffic actually conforms to the protocol the layer 4 port number suggests.
- **Rule Definitions:** User-defined expressions, based on protocol fields and/or protocol-states, which define what actions to take when specific field values are true. Expressions may contain a number of operator types (string, =, >, etc.) based on the data type of the operand. Each Ruledef configuration is consisting of multiple expressions applicable to any of the fields or states supported by the respective analyzers.
- **Rule Bases:** a collection of rule definitions and their associated billing policy. The rule base determines the action to be taken when a rule is matched. It is possible to define a rule definition with different actions.

### Mediation and Charging Methods

To provide maximum flexibility when integrating with billing mediation systems, ECS supports a full range of charging and authorization interfaces.

- **Pre-paid:** In a pre-paid environment, the subscribers pay for service prior to use. While the subscriber is using the service, credit is deducted from subscriber's account until it is exhausted or call ends. The pre-paid accounting server is responsible for authorizing network nodes (GGSNs) to grant access to the user, as well as grant quotas for either time connected or volume used. It is up to the network node to track the quota use, and when these use quotas run low, the network node sends a request to the pre-paid server for more quota.

If the user has not used up the purchased credit, the server grants quota and if no credit is available to the subscriber the call will be disconnected. ECS and DCCA manage this functionality by providing the ability to setup quotas for different services.

Pre-paid quota in ECS is implemented using DIAMETER Credit Control Application (DCCA). DCCA supports the implementation of real-time credit control for a variety of services, such as networks access, messaging services, and download services.

In addition to being a general solution for real-time cost and credit control, DCCA includes these features:

- **Real-time Rate Service Information** - DCCA can verify when end subscribers' accounts are exhausted or expired; or deny additional chargeable events.
- **Support for Multiple Services** - DCCA supports the usage of multiple services within one subscriber session. Multiple Service support includes; 1) ability to identify and process the service or group of services that are subject to different cost structures 2) independent credit control of multiple services in a single credit control sub-session.

Refer to the [Diameter Credit Control Application](#) section for more information.

- **Post-paid:** In a post-paid environment, the subscribers pay after use of the service. A AAA server is responsible for authorizing network nodes (GGSNs) to grant access to the user and a CDR system generates G-CDRs/eG-

CDRs/EDRs/UDRs or Comma Separated Values (CSVs) for billing information on pre-defined intervals of volume or per time.



**Important:** Support for the Enhanced Charging Service requires a service license; the ECS license is included in the P-GW session use license. For more information on ECS, refer to the *Enhanced Charging Service Administration Guide*.

## Content Analysis Support

The Enhanced Charging Service is capable of performing content analysis on packets of many different protocols at different layers of the OSI model.

The ECS content analyzers are able to inspect and maintain state across various protocols at all layers of the OSI stack. ECS system supports, inspects, and analyzes the following protocols:

- IP
- TCP
- UDP
- DNS
- FTP
- TFTP
- SMTP
- POP3
- HTTP
- ICMP
- WAP: WTP and WSP
- Real-Time Streaming: RTP and RTSP
- MMS
- SIP and SDP
- File analysis: examination of downloaded file characteristics (e.g. file size, chunks transferred, etc.) from file transfer protocols such as HTTP and FTP.

Traffic analyzers in enhanced charging subsystem are based on configured rules. Rules used for Traffic analysis analyze packet flows and form usage records. Usage records are created per content type and forwarded to a pre-paid server or to a mediation/billing system. A traffic analyzer performs shallow (Layer 3 and Layer 4) and deep (above Layer 4) packet inspection of the IP packet flows.

The Traffic Analyzer function is able to do a shallow (layer 3 and layer 4) and deep (above layer 4) packet inspection of IP Packet Flows.

It is able to correlate all layer 3 packets (and bytes) with higher layer trigger criteria (e.g. URL detected in a HTTP header) and it is also perform stateful packet inspection to complex protocols like FTP, RTSP, SIP that dynamically open ports for the data path and by this way, user plane payload is differentiated into “categories”.

The Traffic Analyzer works on the application level as well and performs event based charging without the interference of the service platforms.

---

 **Important:** This functionality is available for use with the Enhanced Charging Service which requires a session-use license. For more information on ECS, refer to the *Enhanced Charging Service Administration Guide*.

---

## Content Service Steering

Content Service Steering (CSS) directs selective subscriber traffic into the ECS subsystem (In-line services internal to the system) based on the content of the data presented by mobile subscribers.

CSS uses Access Control Lists (ACLs) to redirect selective subscriber traffic flows. ACLs control the flow of packets into and out of the system. ACLs consist of “rules” (ACL rules) or filters that control the action taken on packets matching the filter criteria.

ACLs are configurable on a per-context basis and applies to a subscriber through either a subscriber profile or an APN profile in the destination context.

---

 **Important:** For more information on CSS, refer to the *Content Service Steering* chapter of the *System Administration Guide*.

 **Important:** For more information on ACLs, refer to the *IP Access Control Lists* chapter of the *System Administration Guide*.

---

## Support for Multiple Detail Record Types

To meet the requirements of standard solutions and at the same time, provide flexible and detailed information on service usage, the Enhanced Charging Service (ECS) provides the following type of usage records:

- Event Detail Records (EDRs)
- Usage Detail Records (UDRs)

ECS provides for the generation of charging data files, which can be periodically retrieved from the system and used as input to a billing mediation system for post-processing. These files are provided in a standard format, so that the impact on the existing billing/mediation system is minimal and at the same time, these records contain all the information required for billing based on the content.

GTPP accounting in ECS allows the collection of counters for different types of data traffic into detail records. The following types of detail records are supported:

- **Event Detail Records (EDRs):** An alternative to standard G-CDRs when the information provided by the G-CDRs is not sufficient to do the content billing. EDRs are generated according to explicit action statements in rule commands that are user-configurable. The EDRs are generated in comma separated values (CSV) format, generated as defined in traffic analysis rules.
- **User Detail Records (UDRs):** Contain accounting information related to a specific mobile subscriber. The fields to be reported in them are user-configurable and are generated on any trigger of time threshold, volume threshold, handoffs, and call termination. The UDRs are generated in comma separated values (CSV) format, generated as defined in traffic analysis rules.

---

 **Important:** This functionality is available for use with the Enhanced Charging Service which requires a session-use license. For more information on ECS, refer to the *Enhanced Charging Service Administration Guide*.

---

## Diameter Credit Control Application

Provides a pre-paid billing mechanism for real-time cost and credit control based on the following **standards**:

- RFC 3588, Diameter Base Protocol, September 2003
- RFC 4006, Diameter Credit-Control Application, August 2005

The Diameter Credit Control Application (DCCA) is used to implement real-time credit-control for a variety of end user services such as network access, Session Initiation Protocol (SIP) services, messaging services, download services etc.

Used in conjunction with ECS, the DCCA interface uses a mechanism to allow the user to be informed of the charges to be levied for a requested service. In addition, there are services such as gaming and advertising that may credit as well as debit from a user account.

DCCA also supports the following:

- **Real-time Rate Service Information:** The ability to verify when end subscribers' accounts are exhausted or expired; or deny additional chargeable events.
- **Support for Multiple Services:** The usage of multiple services within one subscriber session is supported. Multiple Service support includes:
  - The ability to identify and process the service or group of services that are subject to different cost structures.
  - Independent credit control of multiple services in a single credit control sub-session.

---

 **Important:** This functionality is available for use with the Enhanced Charging Service, which requires a session-use license. For more information on ECS, refer to the *Enhanced Charging Service Administration Guide*.

---

## Accept TCP Connections from DCCA Server

This feature allows for peer Diameter Credit Control Application servers to initiate a connection the NGME.

This feature allows peer diameter nodes to connect to the NGME on TCP port 3868 when the diameter server is incapable of receiving diameter incoming diameter requests.

---

 **Important:** For more information on Diameter support, refer to the *AAA and GTPP Interface Administration and Reference*.

---

## Gy Interface Support

The Gy interface enables the wireless operator to implement a standardized interface for real time content based charging with differentiated rates for time based and volume based charging.

As it is based on a quota mechanism, the Gy interface enables the wireless operator to spare expensive Prepaid System resources.

As it enables time-, volume-, and event-based charging models, the Gy interface flexibly enables the operator to implement charging models tailored to their service strategies.

The Gy interface provides a standardized Diameter interface for real time content based charging of data services. It is based on the 3GPP standards and relies on quota allocation.

It 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.

Gy is a Diameter interface. As such, it is implemented atop, and inherits features from, the Diameter Base Protocol. The system supports the applicable Base network and application features, including directly connected, relayed or proxied DCCA servers using TLS or plaintext TCP.

In the simplest possible installation, the system exchanges 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 Cisco implementation is based on the following standards:

- RFC 4006 generic DCCA, including:
  - CCR Initial, Update, and Final signaling
  - ASR and RAR asynchronous DCCA server messages
  - Time, Total-Octets, and Service-Specific-Units quota management
  - Multiple independent quotas using Multiple-Services-Credit-Control
  - Rating-Group for quota-to-traffic association
  - CC-Failure-Handling and CC-Session-Failover features
  - Final-Unit-Action TERMINATE behavior
  - Tariff-Time-Change feature.
- 3GPP TS 32.299 online mode “Gy” DCCA, including:
  - Final-Unit-Action REDIRECT behavior
  - Quota-Holding-Time: This defines a user traffic idle time, on a per category basis, after which the usage is returned and no new quota is explicitly requested
  - Quota-Thresholds: These AVPs define a low value watermark at which new quota will be sought before the quota is entirely gone; the intent is to limit interruption of user traffic.  
These AVPs exist for all quota flavors, for example “Time-Quota-Threshold”.
  - Trigger-Type: This AVP defines a set of events which will induce a re-authentication of the current session and its quota categories.

## Gn/Gp Handoff Support

In LTE deployments, 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. P-GW supports handovers as user equipment (UE) moves across different access technologies.

Cisco's P-GW 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. 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 P-GW supports handoffs between GTPv2 based S5/S8 and GTPv1 based Gn/Gp tunneled connections. In this scenario, the P-GW works as an IP anchor for the EPC.

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

**Important:** For more information on Gn/GP handoffs, refer to *Gn/Gp GGSN/SGSN (GERAN/UTRAN)* in the *Supported Logical Network Interfaces (Reference Points)* section in this chapter.

## IMS Emergency Bearer Handling

With this support, a UE is able to connect to an emergency PDN and make Enhanced 911 (E911) calls while providing the required location information to the Public Safety Access Point (PSAP).

E911 is a telecommunications-based system that is designed to link people who are experiencing an emergency with the public resources that can help. This feature supports E911-based calls across the LTE and IMS networks. In a voice over LTE scenario, the subscriber attaches to a dedicated packet data network (PDN) called EPDN (Emergency PDN) in order to establish a voice over IP connection to the PSAP. Signaling either happens on the default emergency bearer, or signaling and RTP media flow over separate dedicated emergency bearers. Additionally, different than normal PDN attachment that relies on AAA and PCRF components for call establishment, the EPDN attributes are configured locally on the P-GW, which eliminates the potential for emergency call failure if either of these systems is not available.

Emergency bearer services are provided to support IMS emergency sessions. Emergency bearer services are functionalities provided by the serving network when the network is configured to support emergency services. Emergency bearer services are provided to normally attached UEs and to UEs that are in a limited service state (depending on local service regulations, policies, and restrictions). Receiving emergency services in limited service state does not require a subscription.

The standard (refer to 3GPP TS 23.401) has identified four behaviors that are supported:

- Valid UEs only
- Authenticated UEs only
- MSI required, authentication optional
- All UEs

To request emergency services, the UE has the following two options:

- UEs that are in a limited service state (due to attach reject from the network, or since no SIM is present), initiate an ATTACH indicating that the ATTACH is for receiving emergency bearer services. After a successful attach, the services that the network provides the UE is solely in the context of Emergency Bearer Services.
- UEs that camp normally on a cell initiates a normal ATTACH if it requires emergency services. Normal attached UEs initiated a UE Requested PDN Connectivity procedure to request Emergency Bearer Services.

## IP Access Control Lists

IP access control lists allow you to set up rules that control the flow of packets into and out of the system based on a variety of IP packet parameters.

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



**Important:** For more information on IP access control lists, refer to the *IP Access Control Lists* chapter in the *System Administration Guide*.

## IP Address Hold Timers

Also known as address quarantining, this subscriber-level CLI introduces an address hold timer to temporarily buffer a previously assigned IP address from an IP address pool to prevent it from being recycled and reassigned to a new subscriber session. It is especially useful during inter-RAT handovers that sometimes lead to temporary loss of the mobile data session.

This feature provides a higher quality user experience for location-based services where the remote host server needs to reach the mobile device.

## IPv6 Capabilities

Enables increased address efficiency and relieves pressures caused by rapidly approaching IPv4 address exhaustion problem.

The P-GW offers the following IPv6 capabilities:

### Native IPv6 and IPv6 transport

- Support for any combination of IPv4, IPv6 or dual stack IPv4/v6 address assignment from dynamic or static address pools on the P-GW.
- Support for native IPv6 transport and service addresses on PMIPv6 S2a interface. Note that transport on GTP S5/S8 connections in this release is IPv4 based.
- Support for IPv6 transport for outbound traffic over the SGi reference interface to external Packet Data Networks.

### IPv6 Connections to Attached Elements

IPv6 transport and interfaces are supported on all of the following connections:

- Diameter Gx policy signaling interface
- Diameter Gy online charging reference interface
- S6b authentication interface to external 3GPP AAA server
- Diameter Rf offline charging interface
- Lawful Intercept (X1, X2 interfaces)

### Routing and Miscellaneous Features

- OSPFv3
- MP-BGP v6 extensions

- IPv6 flows (Supported on all Diameter QoS and Charging interfaces as well as Inline Services (e.g. ECS))

## Local Break-Out

Provides a standards-based procedure to enable LTE operators to generate additional revenues by accepting traffic from visited subscribers based on roaming agreements with other mobile operators.

Local Breakout is a policy-based forwarding function that plays an important role in inter-provider roaming between LTE service provider networks. Local Breakout is determined by the SLAs for handling roaming calls between visited and home networks. In some cases, it is more beneficial to locally breakout a roaming call on a foreign network to the visited P-W rather than incur the additional transport costs to backhaul the traffic to the Home network.

If two mobile operators have a roaming agreement in place, Local Break-Out enables the visited user to attach to the V-PLMN network and be anchored by the local P-GW in the visited network. The roaming architecture relies on the HSS in the home network and also introduces the concept of the S9 policy signaling interface between the H-PCRF in the H-PLMN and the V-PCRF in the V-PLMN. When the user attaches to the EUTRAN cell and MME (Mobility Management Entity) in the visited network, the requested APN name in the S6a NAS signaling is used by the HSS in the H-PLMN to select the local S-GW (Serving Gateway) and P-GWs in the visited EPC network.

## 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 (Cisco 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.

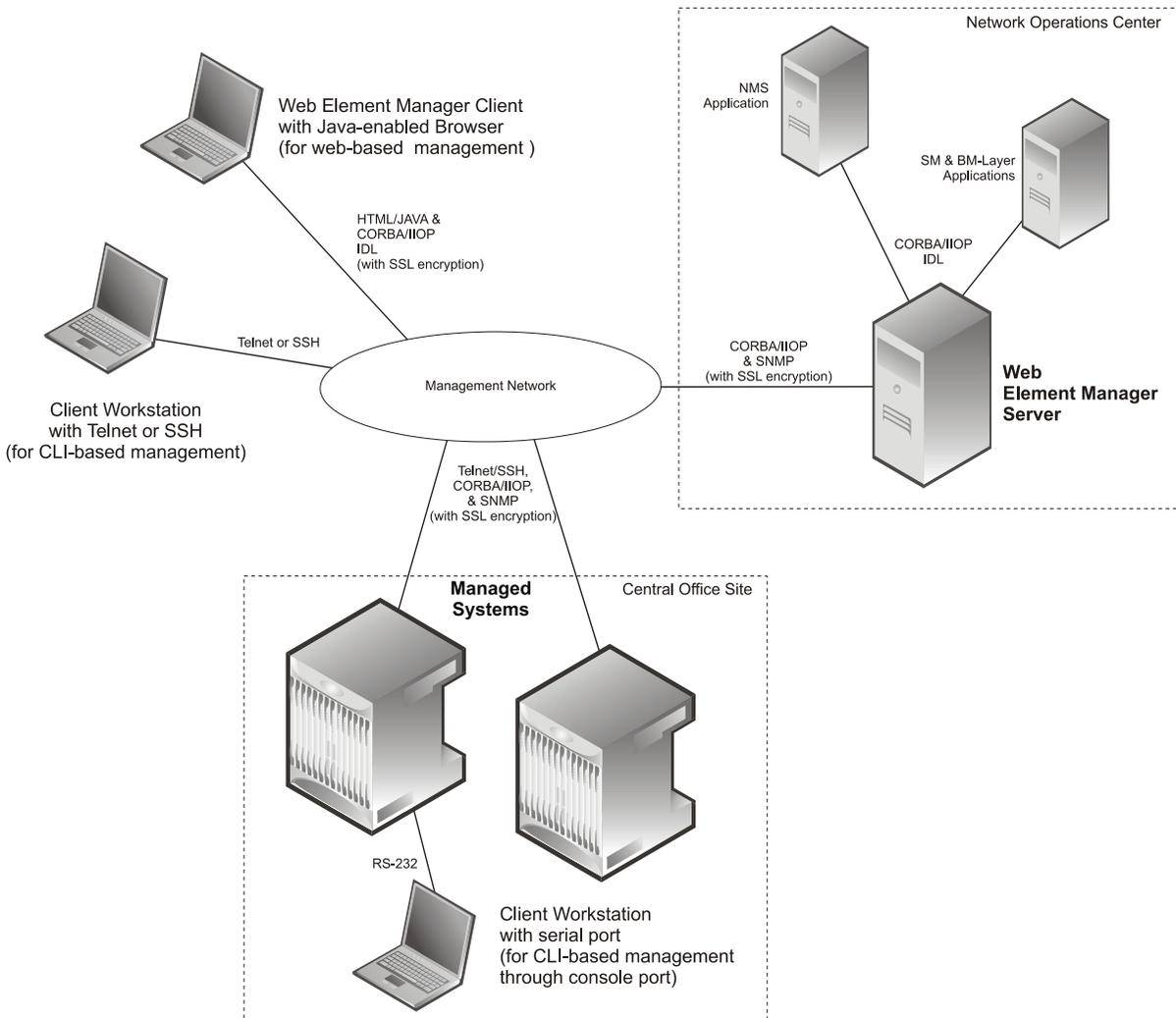
Cisco's O&M module offers comprehensive management capabilities to the operators and enables them to operate the system more efficiently. There are multiple ways to manage the system either locally or remotely using its out-of-band management interfaces.

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 7. Element Management Methods



**Important:** P-GW management functionality is enabled by default for console-based access. For GUI-based management support, refer to the [Web Element Management System](#) section in this chapter.

**Important:** For more information on command line interface based management, refer to the *Command Line Interface Reference*.

## Mobile IP Registration Revocation

Mobile IP registration revocation functionality provides the following benefits:

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

Registration Revocation is a general mechanism whereby either the P-GW or the HSGW providing Mobile IP functionality to the same mobile node can notify the other mobility agent of the termination of a binding. Mobile IP Registration Revocation can be triggered at the HSGW 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 HSGW sessions (sessions that could not be recovered)

---

 **Important:** Registration Revocation functionality is also supported for Proxy Mobile IP. However, only the P-GW can initiate the revocation for Proxy-MIP calls.

 **Important:** For more information on MIP registration revocation support, refer to the *Mobile IP Registration Revocation* appendix in this guide.

---

## Multiple PDN Support

Enables an APN-based user experience that enables separate connections to be allocated for different services including IMS, Internet, walled garden services, or off-deck content services.

The MAG function on the S-GW can maintain multiple PDN or APN connections for the same user session. The MAG runs a single node level Proxy Mobile IPv6 tunnel for all user sessions toward the LMA function of the P-GW. When a user wants to establish multiple PDN connections, the MAG brings up the multiple PDN connections over the same PMIPv6 session to one or more P-GW LMA's. The P-GW in turn allocates separate IP addresses (Home Network Prefixes) for each PDN connection and each one can run one or multiple EPC default & dedicated bearers. To request the various PDN connections, the MAG includes a common MN-ID and separate Home Network Prefixes, APN's and a Handover Indication Value equal to one in the PMIPv6 Binding Updates.

## Non-Optimized e-HRPD to Native LTE (E-UTRAN) Mobility Handover

This feature enables a seamless inter-technology roaming capability in support of dual mode e-HRPD/e-UTRAN access terminals.

The non-optimized inter-technology mobility procedure is rooted at the P-GW as the mobility anchor point for supporting handovers for dual radio technology e-HRPD/E-UTRAN access terminals. To support this type of call handover, the P-GW supports handoffs between the GTP-based S5/S8 (GTPv2-C / GTPv1-U) and PMIPv6 S2a tunneled connections. It also provisions IPv4, IPv6, or dual stack IPv4/IPv6 PDN connections from a common address pool and preserves IP addresses assigned to the UE during inter-technology handover. In the current release, the native LTE (GTP-based) P-GW service address is IPv4-based, while the e-HRPD (PMIP) address is an IPv6 service address.

During the initial network attachment for each APN that the UE connects to, the HSS returns the FQDN of the P-GW for the APN. The MME uses DNS to resolve the P-GW address. When the PDN connection is established in the P-GW, the P-GW updates the HSS with the IP address of the P-GW on PDN establishment through the S6b authentication

process. When the mobile user roams to the e-HRPD network, the HSS returns the IP address of the P-GW in the P-GW Identifier through the STa interface and the call ends up in the same P-GW. The P-GW is also responsible for initiating the session termination on the serving access connection after the call handover to the target network.

During the handover procedure, all dedicated EPS bearers must be re-established. On LTE- handovers to a target e-HRPD access network, the dedicated bearers are initiated by the mobile access terminal. In contrast, on handovers in the opposite direction from e-HRPD to LTE access networks, the dedicated bearers are network initiated through Gx policy interactions with the PCRF server.

Finally, in order to support the inter-technology handovers, the P-GW uses common interfaces and Diameter endpoint addresses for the various reference points:

- S6b: Non-3GPP authentication
- Gx: QoS Policy and Charging
- Rf: Offline Charging

All three types of sessions are maintained during call handovers. The bearer binding will be performed by the HSGW during e-HRPD access and by the P-GW during LTE access. Thus, the Bearer Binding Event Reporting (BBERF) function needs to migrate between the P-GW and the HSGW during the handover. The HSGW establishes a Gxa session during e-HRPD access for bearer binding and releases the session during LTE access. The HSGW also maintains a limited context during the e-HRPD <->LTE handover to reduce latency in the event of a quick handover from the LTE RAN back to the e-HRPD network.



**Important:** For more information on handoff interfaces, refer to the *Supported Logical Network Interfaces (Reference Points)* section in this chapter.

## Online/Offline Charging

The Cisco EPC platform offers support for online and offline charging interactions with external OCS and CGF/CDF servers.

### Online Charging

#### Gy/Ro Reference Interfaces

The StarOS 9.0 online prepaid reference interface provides compatibility with the 3GPP TS 23.203, TS 32.240, TS 32.251 and TS 32.299 specifications. The Gy/Ro reference interface uses Diameter transport and IPv6 addressing. Online charging is a process whereby charging information for network resource usage must be obtained by the network in order for resource usage to occur. This authorization is granted by the Online Charging System (OCS) upon request from the network. The P-GW uses a charging characteristics profile to determine whether to activate or deactivate online charging. Establishment, modification or termination of EPS bearers is generally used as the event trigger on the PCRF to activate online charging PCC rules on the P-GW.

When receiving a network resource usage request, the network assembles the relevant charging information and generates a charging event towards the OCS in real-time. The OCS then returns an appropriate resource usage authorization that may be limited in its scope (e.g. volume of data or duration based). The OCS assigns quotas for rating groups and instructs the P-GW whether to continue or terminate service data flows or IP CAN bearers.

The following Online Charging models and functions are supported:

- Time based charging

- Volume based charging
- Volume and time based charging
- Final Unit Indication and termination or redirection of service data flows when quota is consumed
- Reauthorization triggers to rearm quotas for one or more rating groups using multi-service credit control (MSCC) instances
- Event based charging
- Billing cycle bandwidth rate limiting: Charging policy is enforced through interactions between the PDN GW and Online Charging Server. The charging enforcement point periodically conveys accounting information for subscriber sessions to the OCS and it is debited against the threshold that is established for the charging policy. Subscribers can be assigned a max usage for their tier (gold, silver, bronze for example), the usage can be tracked over a month, week, day, or peak time within a day. When the subscriber exceeds the usage limit, bandwidth is either restricted for a specific time period, or dropped depending on their tier of service.
- Fair usage controls

## Offline Charging

### Ga/Gz Reference Interfaces

The Cisco P-GW supports 3GPP-compliant offline charging as defined in TS 32.251, TS 32.297 and 32.298. Whereas the S-GW generates SGW-CDRs to record subscriber level access to PLMN resources, the P-GW creates PGW-CDRs to record user access to external networks. Additionally, when Gn/Gp interworking with pre-release SGSNs is enabled, the GGSN service on the P-GW records G-CDRs to record user access to external networks.

To provide subscriber level accounting, the Cisco S-GW and P-GWs support integrated Charging Transfer Functions (CTF) and Charging Data Functions (CDF). Each gateway uses Charging-ID's to distinguish between default and dedicated bearers within subscriber sessions. The Ga/Gz reference interface between the CDF and CGF is used to transfer charging records via the GTPP protocol. In a standards based implementation, the CGF consolidates the charging records and transfers them via an FTP/S-FTP connection over the Bm reference interface to a back-end billing mediation server. The Cisco EPC gateways also offer the ability to FTP/S-FTP charging records between the CDF and CGF server. CDR records include information such as Record Type, Served IMSI, ChargingID, APN Name, TimeStamp, Call Duration, Served MSISDN, PLMN-ID, etc. The ASR 5x00 platform offers a local directory to enable temporary file storage and buffer charging records in persistent memory located on a pair of dual redundant RAID hard disks. Each drive includes 147GB of storage and up to 100GB of capacity is dedicated to storing charging records. For increased efficiency it is also possible to enable file compression using protocols such as GZIP. The Offline Charging implementation offers built-in heart beat monitoring of adjacent CGFs. If the Cisco P-GW has not heard from the neighbor CGF within the configurable polling interval, they will automatically buffer the charging records on the local drives until the CGF reactivates itself and is able to begin pulling the cached charging records.

The P-GW supports a Policy Charging Enforcement Function (PCEF) to enable Flow Based Bearer Charging (FBC) via the Gy reference interface to adjunct OCS servers (See Online Charging description above).

### Rf Reference Interface

The Cisco EPC platforms also support the Rf reference interface to enable direct transfer of charging files from the CTF function of the P-GW to external CDF/CGF servers. This interface uses Diameter Accounting Requests (Start, Stop, Interim, and Event) to transfer charging records to the CDF/CGF. Each gateway relies on triggering conditions for reporting chargeable events to the CDF/CGF. Typically as EPS bearers are activated, modified or deleted, charging records are generated. The EPC platforms include information such as Subscription-ID (IMSI), Charging-ID (EPS bearer identifier) and separate volume counts for the uplink and downlink traffic.

## Proxy Mobile IPv6 (S2a)

Provides a mobility management protocol to enable a single LTE-EPC core network to provide the call anchor point for user sessions as the subscriber roams between native EUTRAN and non-native e-HRPD access networks

S2a represents the trusted non-3GPP interface between the LTE-EPC core network and the evolved HRPD network anchored on the HSGW. In the e-HRPD network, network-based mobility provides mobility for IPv6 nodes without host involvement. Proxy Mobile IPv6 extends Mobile IPv6 signaling messages and reuses the HA function (now known as LMA) on the P-GW. This approach does not require the mobile node to be involved in the exchange of signaling messages between itself and the Home Agent. A proxy mobility agent (e.g. MAG function on HSGW) in the network performs the signaling with the home agent and does the mobility management on behalf of the mobile node attached to the network.

The S2a interface uses IPv6 for both control and data. During the PDN connection establishment procedures the P-GW allocates the IPv6 Home Network Prefix (HNP) via Proxy Mobile IPv6 signaling to the HSGW. The HSGW returns the HNP in router advertisement or based on a router solicitation request from the UE. PDN connection release events can be triggered by either the UE, the HSGW or the P-GW.

In Proxy Mobile IPv6 applications the HSGW (MAG function) and P-GW (LMA function) maintain a single shared tunnel and separate GRE keys are allocated in the PMIP Binding Update and Acknowledgement messages to distinguish between individual subscriber sessions. If the Proxy Mobile IP signaling contains Protocol Configuration Options (PCOs) it can also be used to transfer P-CSCF or DNS server addresses

## QoS Bearer Management

Provides a foundation for contributing towards improved Quality of User Experience (QoE) by enabling deterministic end-to-end forwarding and scheduling treatments for different services or classes of applications pursuant to their requirements for committed bandwidth resources, jitter and delay. In this way, each application receives the service treatment that users expect.

An EPS bearer is a logical aggregate of one or more Service Data Flows (SDFs), running between a UE and a P-GW in case of GTP-based S5/S8, and between a UE and HSGW in case of PMIP-based S2a connection. An EPS bearer is the level of granularity for bearer level QoS control in the EPC/E-UTRAN. The Cisco P-GW maintains one or more Traffic Flow Templates (TFT's) in the downlink direction for mapping inbound Service Data Flows (SDFs) to EPS bearers. The P-GW maps the traffic based on the downlink TFT to the S5/S8 bearer. The Cisco PDN GW offers all of the following bearer-level aggregate constructs:

**QoS Class Identifier (QCI):** An operator provisioned value that controls bearer level packet forwarding treatments (e.g. scheduling weights, admission thresholds, queue management thresholds, link layer protocol configuration, etc). The Cisco EPC gateways also support the ability to map the QCI values to DiffServ code points in the outer GTP tunnel header of the S5/S8 connection. Additionally, the platform also provides configurable parameters to copy the DSCP marking from the encapsulated payload to the outer GTP tunnel header.

**Guaranteed Bit Rate (GBR):** A GBR bearer is associated with a dedicated EPS bearer and provides a guaranteed minimum transmission rate in order to offer constant bit rate services for applications such as interactive voice that require deterministic low delay service treatment.

**Maximum Bit Rate (MBR):** The MBR attribute provides a configurable burst rate that limits the bit rate that can be expected to be provided by a GBR bearer (e.g. excess traffic may get discarded by a rate shaping function). The MBR may be greater than or equal to the GBR for a given Dedicated EPS bearer.

**Aggregate Maximum Bit Rate (AMBR):** AMBR denotes a bit rate of traffic for a group of bearers destined for a particular PDN. The Aggregate Maximum Bit Rate is typically assigned to a group of Best Effort service data flows over the Default EPS bearer. That is, each of those EPS bearers could potentially utilize the entire AMBR, e.g. when the other EPS bearers do not carry any traffic. The AMBR limits the aggregate bit rate that can be expected to be provided

by the EPS bearers sharing the AMBR (e.g. excess traffic may get discarded by a rate shaping function). AMBR applies to all Non-GBR bearers belonging to the same PDN connection. GBR bearers are outside the scope of AMBR.

**Policing and Shaping:** The Cisco P-GW offers a variety of traffic conditioning and bandwidth management capabilities. These tools enable usage controls to be applied on a per-subscriber, per-EPS bearer or per-PDN/APN basis. It is also possible to apply bandwidth controls on a per-APN AMBR capacity. These applications provide the ability to inspect and maintain state for user sessions or Service Data Flows (SDFs) within them using shallow L3/L4 analysis or high touch deep packet inspection at L7. Metering of out-of-profile flows or sessions can result in packet discards or reducing the DSCP marking to Best Effort priority. When traffic shaping is enabled the P-GW enqueues the non-conforming session to the provisioned memory limit for the user session. When the allocated memory is exhausted, the inbound/outbound traffic for the user can be transmitted or policed in accordance with operator provisioned policy.

## 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 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 P-GW 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*.

---

## Source IP Address Validation

Insures integrity between the attached subscriber terminal and the PDN GW by mitigating the potential for unwanted spoofing or man-in-the-middle attacks.

The P-GW includes local IPv4/IPv6 address pools for assigning IP addresses to UEs on a per-PDN basis. The P-GW defends its provisioned address bindings by insuring that traffic is received from the host address that it has awareness of. In the event that traffic is received from a non-authorized host, the P- GW includes the ability to block the non-authorized traffic. The P-GW uses the IPv4 source address to verify the sender and the IPv6 source prefix in the case of IPv6.

## Subscriber Level Trace

Provides a 3GPP standards-based session level trace function for call debugging and testing new functions and access terminals in an LTE environment.

As a complement to Cisco's protocol monitoring function, the P-GW supports 3GPP standards based session level trace capabilities to monitor all call control events on the respective monitored interfaces including S5/S8, S2a, SGi, and Gx. The trace can be initiated using multiple methods:

- Management initiation via direct CLI configuration
- Management initiation at HSS with trace activation via authentication response messages over S6a 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 EPC network element buffers the trace activation instructions for the provisioned subscriber in memory using camp-on monitoring. Trace files for active calls are buffered as XML files

using non-volatile memory on the local dual redundant hard drives on the ASR 5x00 platform. 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.

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. In the current release the IPv4 interfaces are used to provide connectivity to the TCE. Trace activation is based on IMSI or IMEI. Once a subscriber level trace request is activated it can be propagated via the S5/S8 signaling to provision the corresponding trace for the same subscriber call on the P-GW. The trace configuration will only be propagated if the P-GW is specified in the list of configured Network Element types received by the S-GW. Trace configuration can be specified or transferred in any of the following message types:

- S5/S8: Create Session Request
- S5/S8: Modify Bearer Request
- S5/S8: Trace Session Activation (New message defined in TS 32.422)

**Performance Goals:** As subscriber level trace is a CPU intensive activity the max number of concurrently monitored trace sessions per Cisco P-GW is 32. Use in a production network should be restricted to minimize the impact on existing services.

## 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 values.

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 to the *Thresholding Configuration Guide*.

---

## UE Time Zone Reporting

This feature enables time-based charging for specialized service tariffs, such as super off-peak billing plans

Time Zone of the UE is associated with UE location (Tracking Area/Routing Area). The UE Time Zone Information Element is an attribute the MME tracks on a Tracking Area List basis and propagates over S11 and S5/S8 signalling to the P-GW.

Time zone reporting can be included in billing records or conveyed in Gx/Gy signaling to external PCRF and OCS servers.

## Virtual APN Support

Virtual APNs allow differentiated services within a single APN.

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

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

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

# Features and Functionality - Inline Service Support

This section describes the features and functions of inline services supported on the P-GW. These services require additional licenses to implement the functionality.

This section describes the following features:

- [Content Filtering](#)
- [Header Enrichment: Header Insertion and Encryption](#)
- [Mobile Video Gateway](#)
- [Network Address Translation \(NAT\)](#)
- [Peer-to-Peer Detection](#)
- [Personal Stateful Firewall](#)
- [Traffic Performance Optimization \(TPO\)](#)

## Content Filtering

The Cisco P-GW offers two variants of network-controlled content filtering / parental control services. Each approach leverages the native DPI capabilities of the platform to detect and filter events of interest from mobile subscribers based on HTTP URL or WAP/MMS URI requests:

- **Integrated Content Filtering:** A turnkey solution featuring a policy enforcement point and category based rating database on the Cisco P-GW. An offboard AAA or PCRF provides the per-subscriber content filtering information as subscriber sessions are established. The content filtering service uses DPI to extract URLs or URIs in HTTP request messages and compares them against a static rating database to determine the category match. The provisioned policy determines whether individual subscribers are entitled to view the content.
- **Content Filtering ICAP Interface:** This solution is appropriate for mobile operators with existing installations of Active Content Filtering external servers. The service continues to harness the DPI functions of the ASR 5x00 platform to extract events of interest. However in this case, the extracted requests are transferred via the Integrated Content Adaptation Protocol (ICAP) with subscriber identification information to the external ACF server which provides the category rating database and content decision functions.

## Integrated Adult Content Filter

Provides a value-added service to prevent unintended viewing of objectionable content that exploits underage children. Content Filtering offers mobile operators a way to increase data ARPU and subscriber retention through a network-based solution for parental controls and content filtering. The integrated solution enables a single policy decision and enforcement point thereby streamlining the number of signaling interactions with external AAA/Policy Manager servers. When used in parallel with other services such as Enhanced Content Charging (ECS) it increases billing accuracy of charging records by insuring that mobile subscribers are only charged for visited sites they are allowed to access.

The Integrated Adult Content Filter is a subscriber-aware inline service provisioned on an ASR 5x00 running P-GW services. Integrated Content Filtering utilizes the local DPI engine and harnesses a distributed software architecture that scales with the number of active P-GW sessions on the system.

Content Filtering policy enforcement is the process of deciding if a subscriber should be able to receive some content. Typical options are to allow, block, or replace/redirect the content based on the rating of the content and the policy

defined for that content and subscriber. The policy definition is transferred in an authentication response from a AAA server or Diameter policy message via the Gx reference interface from an adjunct PCRF. The policy is applied to subscribers through rulebase or APN/Subscriber configuration. The policy determines the action to be taken on the content request on the basis of its category. A maximum of one policy can be associated with a rulebase.

## ICAP Interface

Provides a value-added service to prevent unintended viewing of objectionable content that exploits underage children. Content Filtering offers mobile operators a way to increase data ARPU and subscriber retention through a network-based solution for parental controls and content filtering. The Content Filtering ICAP solution is appropriate for operators with existing installations of Active Content Filtering servers in their networks.

The Enhanced Charging Service (ECS) for the P-GW provides a streamlined Internet Content Adaptation Protocol (ICAP) interface to leverage the Deep Packet Inspection (DPI) to enable external Application Servers to provide their services without performing the DPI functionality and without being inserted in the data flow. The ICAP interface may be attractive to mobile operators that prefer to use an external Active Content Filtering (ACF) Platform. If a subscriber initiates a WAP (WAP1.x or WAP2.0) or Web session, the subsequent GET/POST request is detected by the deep packet inspection function. The URL of the GET/POST request is extracted by the local DPI engine on the ASR 5x00 platform and passed, along with subscriber identification information and the subscriber request, in an ICAP message to the Application Server (AS). The AS 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 the GET/POST message. Depending upon the response received from the ACF server, the P-GW either passes the request unmodified or discards the message and responds to the subscriber with the appropriate redirection or block message.

## Header Enrichment: Header Insertion and Encryption

Header enrichment provides a value-added capability for mobile operators to monetize subscriber intelligence to include subscriber-specific information in the HTTP requests to application servers.

Extension header fields (x-header) are the fields that can be added to headers of a protocol for a specific purpose. The enriched header allows additional entity-header fields to be defined without changing the protocol, but these fields cannot be assumed to be recognizable by the recipient. Unrecognized fields should be ignored by the recipient and must be forwarded by transparent proxies.

Extension headers can be supported in HTTP/WSP GET and POST request packets. The Enhanced Charging Service (ECS) for the P-GW offers APN-based configuration and rules to insert x-headers in HTTP/WSP GET and POST request packets. The charging action associated with the rules will contain the list of x-headers to be inserted in the packets. Protocols supported are HTTP, WAP 1.0 and WAP 2.0 GET, and POST messages.



**Important:** For more information on ECS, see the *Enhanced Charging Service Administration Guide*.

The data passed in the inserted HTTP header attributes is used by end application servers (also known as Upsell Servers) to identify subscribers and session information. These servers provide information customized to that specific subscriber.

The Cisco P-GW can include the following information in the http header:

- User-customizable, arbitrary text string
- Subscriber's MSISDN (the RADIUS calling-station-id, in clear text)
- Subscriber's IMSI
- Subscriber's IP address

- S-GW IP address (in clear text)

X-Header encryption enhances the header enrichment feature by increasing the number of fields that can be supported and through encryption of the fields before inserting them.

The following limitations to insertion of x-header fields in WSP headers apply:

- x-header fields are not inserted in IP fragmented packets.
- In case of concatenated request, x-header fields are only inserted in first GET or POST request (if rule matches for the same). X-header fields are not inserted in the second or later GET/POST requests in the concatenated requests. For example, if there is ACK+GET in packet, x-header is inserted in the GET packet. However, if GET1+GET2 is present in the packet and rule matches for GET2 and not GET1 x-header is still inserted in GET2. In case of GET+POST also, x-header is not inserted in POST.
- In case of CO, x-header fields are not inserted if the WTP packets are received out of order (even after proper reordering).
- If route to MMS is present, x-headers are not inserted.
- x-headers are not inserted in WSP POST packet when header is segmented. This is because POST contains header length field which needs to be modified after addition of x-headers. In segmented WSP headers, header length field may be present in one packet and header may complete in another packet.

## Mobile Video Gateway

The Cisco ASR 5x00 chassis provides mobile operators with a flexible solution that functions as a Mobile Video Gateway in 2.5G, 3G, and 4G wireless data networks.

The Cisco Mobile Video Gateway consists of new software for the ASR 5x00. The Mobile Video Gateway is the central component of the Cisco Mobile Videoscape. It employs a number of video optimization techniques that enable mobile operators to enhance the video experience for their subscribers while optimizing the performance of video content transmission through the mobile network.

The Mobile Video Gateway features and functions include:

- DPI (Deep Packet Inspection) to identify subscriber requests for video vs. non-video content
- Transparent video re-addressing to the Cisco CAE (Content Adaptation Engine) for retrieval of optimized video content
- CAE load balancing of HTTP video requests among the CAEs in the server cluster
- Video optimization policy control for tiered subscriber services
- Video white-listing, which excludes certain video clips from video optimization
- Video pacing for “just in time” video downloading
- TCP link monitoring
- Dynamic inline transrating
- Dynamically-enabled TCP proxy
- Traffic performance optimization
- N+1 redundancy support
- SNMP traps and alarms (threshold crossing alerts)
- Mobile video statistics
- Bulk statistics for mobile video

The Cisco CAE is an optional component of the Cisco Mobile Videoscape. It runs on the Cisco UCS (Unified Computing System) platform and functions in a UCS server cluster to bring additional video optimization capabilities to the Mobile Videoscape. For information about the features and functions of the Cisco CAE, see the CAE product documentation.

---

 **Important:** For more information on the Mobile Video Gateway, refer to the *Mobile Video Gateway Administration Guide*.

---

## Network Address Translation (NAT)

NAT translates non-routable private IP address(es) to routable public IP address(es) from a pool of public IP addresses that have been designated for NAT. This enables to conserve on the number of public IP addresses required to communicate with external networks, and ensures security as the IP address scheme for the internal network is masked from external hosts, and each outgoing and incoming packet goes through the translation process.

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

NAT can be used to perform address translation for simple IP and mobile IP. NAT can be selectively applied/denied to different flows (5-tuple connections) originating from subscribers based on the flows' L3/L4 characteristics—Source-IP, Source-Port, Destination-IP, Destination-Port, and Protocol.

NAT supports the following mappings:

- One-to-One
- Many-to-One

---

 **Important:** For more information on NAT, refer to the *Network Address Translation Administration Guide*.

---

## NAT64 Support

This feature helps facilitate the co-existence and gradual transition to IPv6 addressingscheme in the networks.

With the dwindling IPv4 public address space and the growing need for more routable addresses, service providers and enterprises will continue to build and roll out IPv6 networks. However, because of the broad scale IPv4 deployment, it is not practical that the world changes to IPv6 overnight. There is need to protect the IPv4 investment combined with the need to expand and grow the network will force IPv4 and IPv6 networks to co-exist together for a considerable period of time and keep end-user experience seamless.

The preferred approaches are to run dual stacks (both IPv4 and IPv6) on the end hosts, dual stack routing protocols, and dual stack friendly applications. If all of the above is available, then the end hosts will communicate natively using IPv6 or IPv4 (using NAT). Tunneling through the IPv4 or IPv6 is the next preferred method to achieve communication wherever possible. When all these options fail, translation is recommended.

Stateful NAT64 is a mechanism for translating IPv6 packets to IPv4 packets and vice-versa. The system supports a Stateful NAT64 translator based on IETF Behave WG drafts whose framework is described in draft-ietf-behave-v6v4-framework-10. Stateful NAT64 is available as part of the existing NAT licenses from the current system implementation. The NAT44 and NAT64 will co-exist on the chassis and share the resources needed for NATing.

## Peer-to-Peer Detection

Allows operators to identify P2P traffic in the network and applying appropriate controlling functions to ensure fair distribution of bandwidth to all subscribers.

Peer-to-Peer (P2P) is a term used in two slightly different contexts. At a functional level, it means protocols that interact in a peering manner, in contrast to client-server manner. There is no clear differentiation between the function of one node or another. Any node can function as a client, a server, or both—a protocol may not clearly differentiate between the two. For example, peering exchanges may simultaneously include client and server functionality, sending and receiving information.

Detecting peer-to-peer protocols requires recognizing, in real time, some uniquely identifying characteristic of the protocols. Typical packet classification only requires information uniquely typed in the packet header of packets of the stream(s) running the particular protocol to be identified. In fact, many peer-to-peer protocols can be detected by simple packet header inspection. However, some P2P protocols are different, preventing detection in the traditional manner. This is designed into some P2P protocols to purposely avoid detection. The creators of these protocols purposely do not publish specifications. A small class of P2P protocols is stealthier and more challenging to detect. For some protocols no set of fixed markers can be identified with confidence as unique to the protocol.

Operators care about P2P traffic because of the behavior of some P2P applications (for example, Bittorrent, Skype, and eDonkey). Most P2P applications can hog the network bandwidth such that 20% P2P users can generate as much as traffic generated by the rest 80% non-P2P users. This can result into a situation where non-P2P users may not get enough network bandwidth for their legitimate use because of excess usage of bandwidth by the P2P users. Network operators need to have dynamic network bandwidth / traffic management functions in place to ensure fair distributions of the network bandwidth among all the users. And this would include identifying P2P traffic in the network and applying appropriate controlling functions to the same (for example, content-based premium billing, QoS modifications, and other similar treatments).

Cisco's P2P detection technology makes use of innovative and highly accurate protocol behavioral detection techniques.



**Important:** For more information on peer-to-peer detection, refer to the *Application Detection and Control Administration Guide*.

## Personal Stateful Firewall

The Personal Stateful Firewall is an in-line service feature that inspects subscriber traffic and performs IP session-based access control of individual subscriber sessions to protect the subscribers from malicious security attacks.

The Personal Stateful Firewall supports stateless and stateful inspection and filtering based on the configuration.

In stateless inspection, the firewall inspects a packet to determine the 5-tuple—source and destination IP addresses and ports, and protocol—information contained in the packet. This static information is then compared against configurable rules to determine whether to allow or drop the packet. In stateless inspection the firewall examines each packet individually, it is unaware of the packets that have passed through before it, and has no way of knowing if any given packet is part of an existing connection, is trying to establish a new connection, or is a rogue packet.

In stateful inspection, the firewall not only inspects packets up through the application layer / layer 7 determining a packet's header information and data content, but also monitors and keeps track of the connection's state. For all active connections traversing the firewall, the state information, which may include IP addresses and ports involved, the sequence numbers and acknowledgement numbers of the packets traversing the connection, TCP packet flags, etc. is maintained in a state table. Filtering decisions are based not only on rules but also on the connection state established by prior packets on that connection. This enables to prevent a variety of DoS, DDoS, and other security violations. Once a connection is torn down, or is timed out, its entry in the state table is discarded.

The Enhanced Charging Service (ECS) / Active Charging Service (ACS) in-line service is the primary vehicle that performs packet inspection and charging. For more information on ECS, see the *Enhanced Charging Service Administration Guide*.

---

 **Important:** For more information on Personal Stateful Firewall, refer to the *Personal Stateful Firewall Administration Guide*.

---

## Traffic Performance Optimization (TPO)

Though TCP is a widely accepted protocol in use today, it is optimized only for wired networks. Due to inherent reliability of wired networks, TCP implicitly assumes that any packet loss is due to network congestion and consequently invokes congestion control measures. However, wireless links are known to experience sporadic and usually temporary losses due to several reasons, including the following, which also trigger TCP congestion control measures resulting in poor TCP performance.

Reasons for delay variability over wireless links include:

- Channel fading effect, subscriber mobility, and other transient conditions
- Link-layer retransmissions
- Handoffs between neighboring cells
- Intermediate nodes, such as SGSN and e-NodeB, implementing scheduling policies tuned to deliver better QoS for select services; resulting in variable delay in packet delivery for other services

The TPO inline service uses a combination of TCP and HTTP optimization techniques to improve TCP performance over wireless links.

---

 **Important:** For more information on TPO, refer to the *Traffic Performance Optimization Administration Guide*.

---

# Features and Functionality - External Application Support

This section describes the features and functions of external applications supported on the P-GW. These services require additional licenses to implement the functionality.

This section describes the following feature(s):

- [Web Element Management System](#)

## Web Element Management System

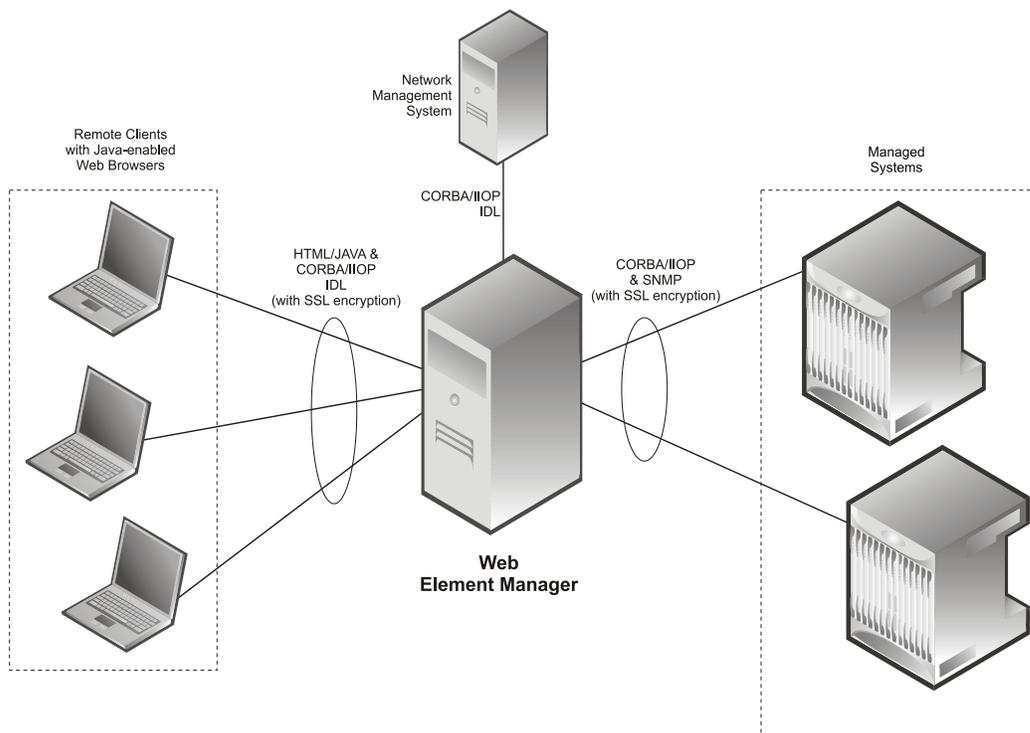
Provides a graphical user interface (GUI) for performing fault, configuration, accounting, performance, and security (FCAPS) management of the ASR 5x00.

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 8. Web Element Manager Network Interfaces**





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

---

# Features and Functionality - Optional Enhanced Feature Software

This section describes the optional enhanced features and functions for the P-GW service.

Each of the following features requires the purchase of an additional license to implement the functionality with the P-GW service.

---

 **Important:** 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 section describes the following features:

- [Always-On Licensing](#)
- [GRE Protocol Interface Support](#)
- [Inter-Chassis Session Recovery](#)
- [IP Security \(IPSec\) Encryption](#)
- [L2TP LAC Support](#)
- [Lawful Intercept](#)
- [Layer 2 Traffic Management \(VLANs\)](#)
- [Local Policy Decision Engine](#)
- [MPLS Forwarding with LDP](#)
- [NEMO Service Supported](#)
- [Session Recovery Support](#)
- [Smartphone Tethering Detection Support](#)
- [Traffic Policing and Shaping](#)
- [User Location Information Reporting](#)

## Always-On Licensing

Use of Always On Licensing requires that a valid license key be installed. Contact your Cisco account representative for information on how to obtain a license.

Traditionally, transactional models have been based on registered subscriber sessions. In an “always-on” deployment model, however, the bulk of user traffic is registered all of the time. Most of these registered subscriber sessions are idle a majority of the time. Therefore, Always-On Licensing charges only for connected-active subscriber sessions.

A connected-active subscriber session would be in “ECM Connected state,” as specified in 3GPP TS 23.401, with a data packet sent/received within the last one minute (on average). This transactional model allows providers to better manage and achieve more predictable spending on their capacity as a function of the Total Cost of Ownership (TCO).

## GRE Protocol Interface Support

Use of GRE Interface Tunneling requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

The P-GW supports GRE generic tunnel interfaces in accordance with RFC 2784, Generic Routing Encapsulation (GRE). The GRE protocol allows mobile users to connect to their enterprise networks through GRE tunnels.

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.



**Important:** For more information on GRE protocol interface support, refer to the *GRE Protocol Interface* appendix in this guide.

---

## Inter-Chassis Session Recovery

Use of Interchassis Session Recovery requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

The ASR 5x00 provides industry leading carrier class redundancy. The system 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 PSC/PSC2 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 PSC/PSC2 failure will cause a PSC switchover and all established sessions for supported call-types are recovered without any loss of session.

Even though Cisco 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 MME 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 Interchassis 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 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 Messages**

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 to the *Interchassis Session Recovery* chapter in the *System Administration Guide*.

---

## IP Security (IPSec) Encryption

Use of Network Domain Security requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

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

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

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

---

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

---

## L2TP LAC Support

Use of L2TP LAC requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

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 P-GW and the corporation, an L2TP tunnel must be setup in the P-GW 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 P-GW and benefits from dynamic resource allocation and distributed message and data processing.

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 to the *L2TP Access Concentrator* appendix in this guide.

---

## Lawful Intercept

The feature use license for Lawful Intercept on the P-GW is included in the P-GW session use license.

The Cisco Lawful Intercept feature is supported on the P-GW. Lawful Intercept is a licensed-enabled, standards-based feature that provides telecommunications service providers with a mechanism to assist law enforcement agencies in monitoring suspicious individuals for potential illegal activity. For additional information and documentation on the Lawful Intercept feature, contact your Cisco account representative.

## Layer 2 Traffic Management (VLANs)

Use of Layer 2 Traffic Management requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

Virtual LANs (VLANs) provide greater flexibility in the configuration and use of contexts and services.

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

---

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

---

## Local Policy Decision Engine

Use of the Local Policy Decision Engine requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

The Local Policy Engine is an event-driven rules engine that offers Gx-like QoS and policy controls to enable user or application entitlements. As the name suggests, it is designed to provide a subset of a PCRF in cases where an operator elects not to use a PCRF or scenarios where connections to an external PCRF are disrupted. Local policies are used to control different aspects of a session like QoS, data usage, subscription profiles, and server usage by means of locally defined policies. A maximum of 1,024 local policies can be provisioned on a P-GW system.

Local policies are triggered when certain events occur and the associated conditions are satisfied. For example, when a new call is initiated, the QoS to be applied for the call could be decided based on the IMSI, MSISDN, and APN.

Potential uses cases for the Local Policy Decision Engine include:

- Disaster recovery data backup solution in the event of a loss of PCRF in a mobile core network.
- Dedicated bearer establishment for emergency voice calls.
- Network-initiated bearer establishment on LTE to non-3GPP inter-domain handovers.

---

 **Important:** For more information on configuring the Local Policy Decision Engine, refer to the *Configuring Local QoS Policy* section in the *PDN Gateway Configuration* chapter of this guide.

---

## MPLS Forwarding with LDP

Use of MPLS requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

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.

MPLS 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 the 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, the MPLS backbone automatically negotiates routes using the labels binded with the IP packets. Cisco P-GW 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 P-GW.

---

 **Important:** For more information on MPLS support, refer to the *Multi-Protocol Label Switching (MPLS) Support* appendix in this guide.

---

## NEMO Service Supported

Use of NEMO requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

The P-GW may be configured to enable or disable Network Mobility (NEMO) service.

When enabled, the system includes NEMO support for a Mobile IPv4 Network Mobility (NEMO-HA) on the P-GW platform to terminate Mobile IPv4 based NEMO connections from Mobile Routers (MRs) that attach to an Enterprise PDN. The NEMO functionality allows bi-directional communication that is application-agnostic between users behind the MR and users or resources on Fixed Network sites.

The same NEMO4G-HA service and its bound Loopback IP address supports NEMO connections whose underlying PDN connection comes through GTP S5 (4G access) or PMIPv6 S2a (eHRPD access).



**Important:** For more information on NEMO support, refer to the *Network Mobility (NEMO)* chapter in this guide.

---

## Session Recovery Support

The feature use license for Session Recovery on the P-GW is included in the P-GW session use license.

Session recovery provides seamless failover and reconstruction of subscriber session information in the event of a hardware or software fault within the system preventing a fully connected user session from being disconnected.

In the telecommunications industry, over 90 percent of all equipment failures are software-related. With robust hardware failover and redundancy protection, any card-level hardware failures on the system can quickly be corrected. However, software failures can occur for numerous reasons, many times without prior indication. StarOS Release 9.0 adds the ability to support stateful intra-chassis session recovery for P-GW sessions.

When session recovery occurs, the system reconstructs the following subscriber information:

- Data and control state information required to maintain correct call behavior
- Subscriber data statistics that are required to ensure that accounting information is maintained
- A best-effort attempt to recover various timer values such as call duration, absolute time, and others

Session recovery is also useful for in-service software patch upgrade activities. If session recovery is enabled during the software patch upgrade, it helps to preserve existing sessions on the active PSC/PSC2 during the upgrade process.



**Important:** For more information on session recovery support, refer to the *Session Recovery* chapter in the *System Administration Guide*.

---

## Smartphone Tethering Detection Support

Use of Smartphone Tethering Detection requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

On the P-GW, using the inline heuristic detection mechanism, it is now possible to detect and differentiate between the traffic from the mobile device and a tethered device connected to the mobile device.

## Traffic Policing and Shaping

Use of Per-Subscriber Traffic Policing/Shaping requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

Traffic policing and shaping allows you to manage bandwidth usage on the network and limit bandwidth allowances to subscribers. Shaping allows you to buffer excesses to be delivered at a later time.

### Traffic Policing

Traffic policing enables the configuring and enforcing of bandwidth limitations on individual subscribers and/or APNs 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.



**Important:** For more information on traffic policing and shaping, refer to the *Traffic Policing and Shaping* appendix in this guide.

## User Location Information Reporting

Use of User Location Information (ULI) Reporting requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

ULI Reporting allows the eNodeB to report the location of a UE to the MME, when requested by a P-GW.

The following procedures are used over the S1-MME interface to initiate and stop location reporting between the MME and eNodeB:

- **Location Reporting Control:** The purpose of Location Reporting Control procedure is to allow the MME to request that the eNodeB report where the UE is currently located. This procedure uses UE-associated signaling.
- **Location Report Failure Indication:** The Location Report Failure Indication procedure is initiated by an eNodeB in order to inform the MME that a Location Reporting Control procedure has failed. This procedure uses UE-associated signalling.
- **Location Report:** The purpose of Location Report procedure is to provide the UE's current location to the MME. This procedure uses UE-associated signalling.

The start/stop trigger for location reporting for a UE is reported to the MME by the S-GW over the S11 interface. The Change Reporting Action (CRA) Information Element (IE) is used for this purpose. The MME updates the location to the S-GW using the User Location Information (ULI) IE.

The following S11 messages are used to transfer CRA and ULI information between the MME and S-GW:

- **Create Session Request:** The ULI IE is included for E-UTRAN Initial Attach and UE-requested PDN Connectivity procedures. It includes ECGI and TAI. The MME includes the ULI IE for TAU/ X2-Handover procedure if the P-GW has requested location information change reporting and the MME support location information change reporting. The S-GW includes the ULI IE on S5/S8 exchanges if it receives the ULI from the MME. If the MME supports change reporting, it sets the corresponding indication flag in the Create Session Request message.
- **Create Session Response:** The CRA IE in the Create Session Response message can be populated by the S-GW to indicate the type of reporting required.
- **Create Bearer Request:** The CRA IE is included with the appropriate Action field if the Location Change Reporting mechanism is to be started or stopped for the subscriber in the MME.
- **Modify Bearer Request:** The MME includes the ULI IE for TAU/Handover procedures and UE-initiated Service Request procedures if the P-GW has requested location information change reporting and the MME supports location information change reporting. The S-GW includes this IE on S5/S8 exchanges if it receives the ULI from the MME.
- **Modify Bearer Response:** The CRA IE is included with the appropriate Action field if the Location Change Reporting mechanism is to be started or stopped for the subscriber in the MME.
- **Delete Session Request:** The MME includes the ULI IE for the Detach procedure if the P-GW has requested location information change reporting and MME supports location information change reporting. The S-GW includes this IE on S5/S8 exchanges if it receives the ULI from the MME.
- **Update Bearer Request:** The CRA IE is included with the appropriate Action field if the Location Change Reporting mechanism is to be started or stopped for the subscriber in the MME.
- **Change Notification Request:** If no existing procedure is running for a UE, a Change Notification Request is sent upon receipt of an S1-AP location report message. If an existing procedure is running, one of the following messages reports the ULI:
  - Create Session Request
  - Create Bearer Response

- Modify Bearer Request
- Update Bearer Response
- Delete Bearer Response
- Delete Session Request

If an existing Change Notification Request is pending, it is aborted and a new one is sent.



**Important:** Information on configuring User Location Information (ULI) Reporting support is located in the *Configuring Optional Features on the MME* section of the *Mobility Management Entity Configuration* chapter in the *Mobility Management Entity Administration Guide*.

---

## How the PDN Gateway Works

This section provides information on the function of the P-GW in an EPC E-UTRAN network and presents call procedure flows for different stages of session setup and disconnect.

The P-GW supports the following network flows:

- [PMIPv6 PDN Gateway Call Session Procedures in an eHRPD Network](#)
- [GTP PDN Gateway Call Session Procedures in an LTE-SAE Network](#)

## PMIPv6 PDN Gateway Call/Session Procedures in an eHRPD Network

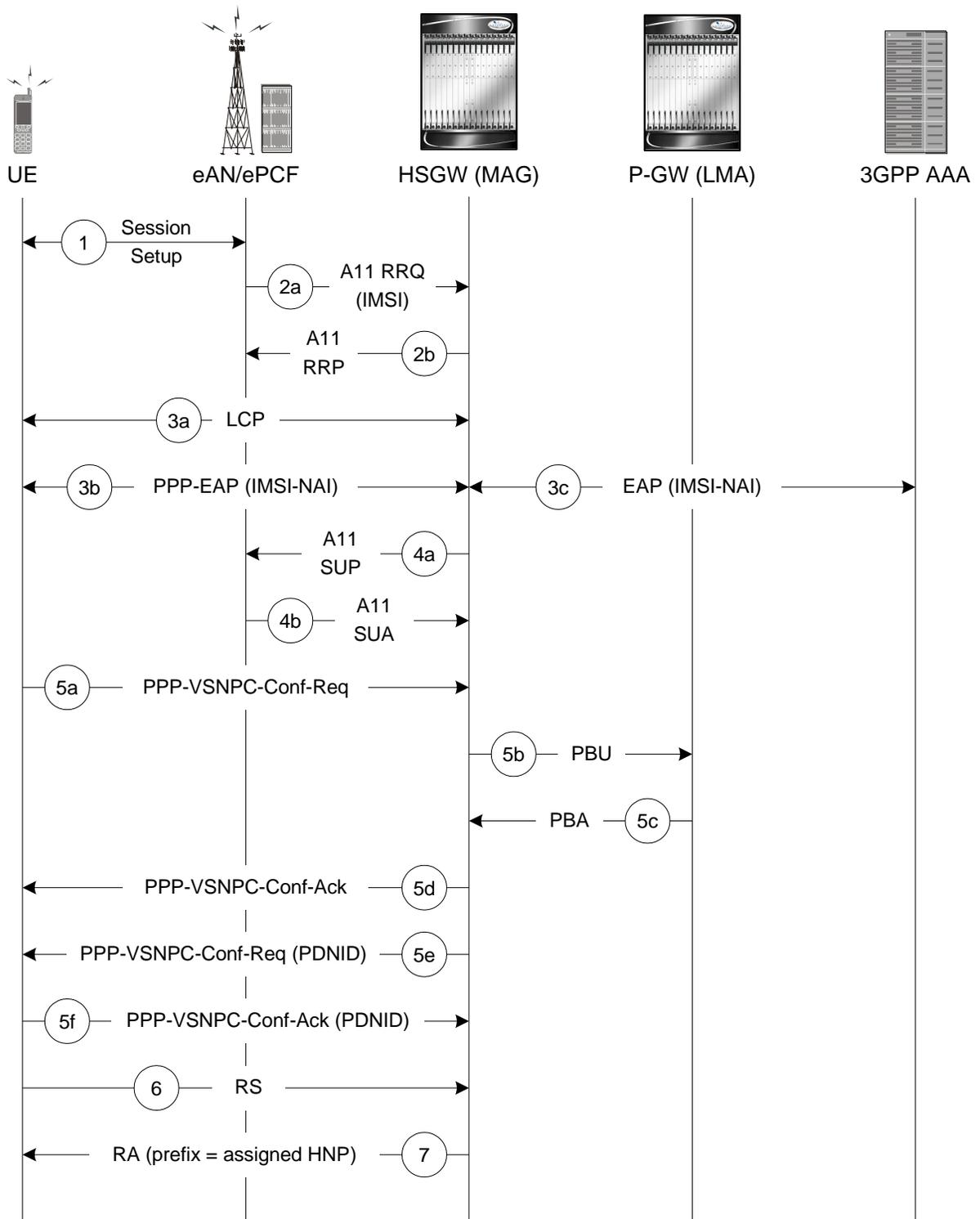
The following topics and procedure flows are included:

- [Initial Attach with IPv6/IPv4 Access](#)
- [PMIPv6 Lifetime Extension without Handover](#)
- [PDN Connection Release Initiated by UE](#)
- [PDN Connection Release Initiated by HSGW](#)
- [PDN Connection Release Initiated by P-GW](#)

### Initial Attach with IPv6/IPv4 Access

This section describes the procedure of initial attach and session establishment for a subscriber (UE).

Figure 9. Initial Attach with IPv6/IPv4 Access Call Flow



**Table 2. Initial Attach with IPv6/IPv4 Access Call Flow Description**

Step	Description
1	The subscriber (UE) attaches to the eHRPD network.
2a	The eAN/PCF sends an A11 RRQ to the HSGW. The eAN/PCF includes the true IMSI of the UE in the A11 RRQ.
2b	The HSGW establishes A10s and respond back to the eAN/PCF with an A11 RRP.
3a	The UE performs LCP negotiation with the HSGW over the established main A10.
3b	The UE performs EAP over PPP.
3c	EAP authentication is completed between the UE and the 3GPP AAA. During this transaction, the HSGW receives the subscriber profile from the AAA server.
4a	After receiving the subscriber profile, the HSGW sends the QoS profile in A11 Session Update Message to the eAN/PCF.
4b	The eAN/PCF responds with an A11 Session Update Acknowledgement (SUA).
5a	The UE initiates a PDN connection by sending a PPP-VSNCP-Conf-Req message to the HSGW. The message includes the PDNID of the PDN, APN, PDN-Type=IPv6/[IPv4], PDSN-Address and, optionally, PCO options the UE is expecting from the network.
5b	The HSGW sends a PBU to the P-GW.
5c	The P-GW processes the PBU from the HSGW, assigns an HNP for the connection and responds back to the HSGW with PBA.
5d	The HSGW responds to the VSNCP Conf Req with a VSNCP Conf Ack.
5e	The HSGW sends a PPP-VSNCP-Conf-Req to the UE to complete PPP VSNCP negotiation.
5f	The UE completes VSNCP negotiation by returning a PPP-VSNCP-Conf-Ack.
6	The UE optionally sends a Router Solicitation (RS) message.
7	The HSGW sends a Router Advertisement (RA) message with the assigned Prefix.

## PMIPv6 Lifetime Extension without Handover

This section describes the procedure of a session registration lifetime extension by the P-GW without the occurrence of a handover.

Figure 10. PMIPv6 Lifetime Extension (without handover) Call Flow

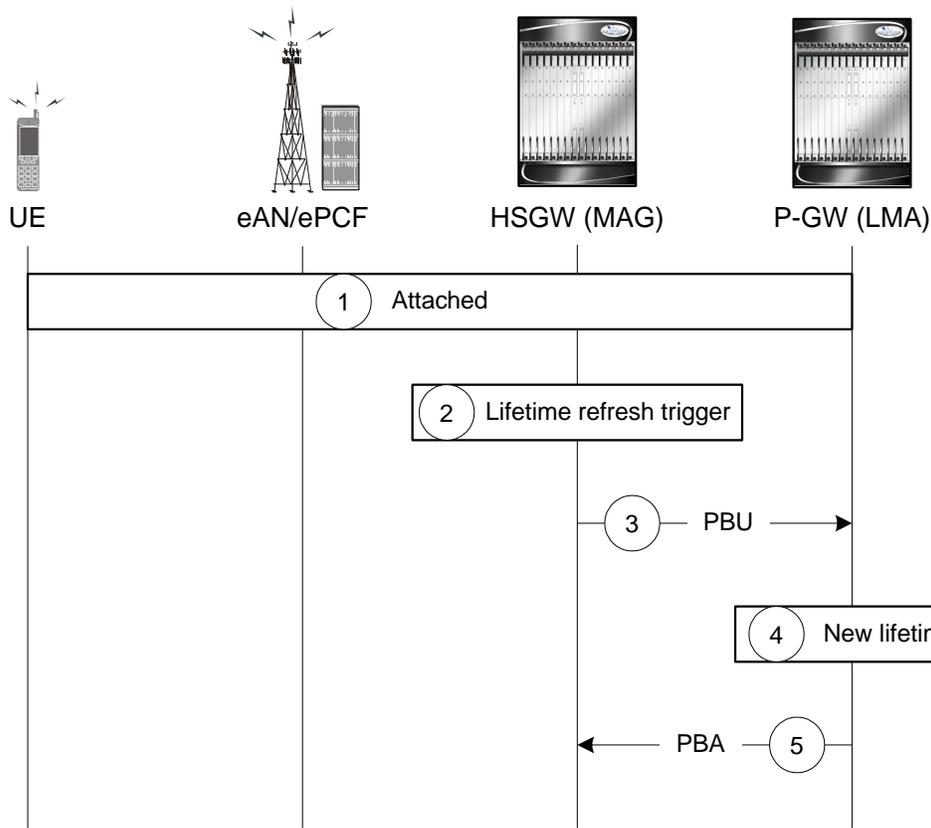


Table 3. PMIPv6 Lifetime Extension (without handover) Call Flow Description

Step	Description
1	The UE is attached to the EPC and has a PDN connection with the P-GW where PDNID=x and an APN with assigned HNP.
2	The HSGW MAG service registration lifetime nears expiration and triggers a renewal request for the LMA.
3	The MAG service sends a Proxy Binding Update (PBU) to the P-GW LMA service with the following attributes: Lifetime, MNID, APN, ATT=HRPD, HNP.
4	The P-GW LMA service updates the Binding Cache Entry (BCE) with the new granted lifetime.
5	The P-GW responds with a Proxy Binding Acknowledgement (PBA) with the following attributes: Lifetime, MNID, APN.

### PDN Connection Release Initiated by UE

This section describes the procedure of a session release by the UE.

Figure 11. PDN Connection Release by the UE Call Flow

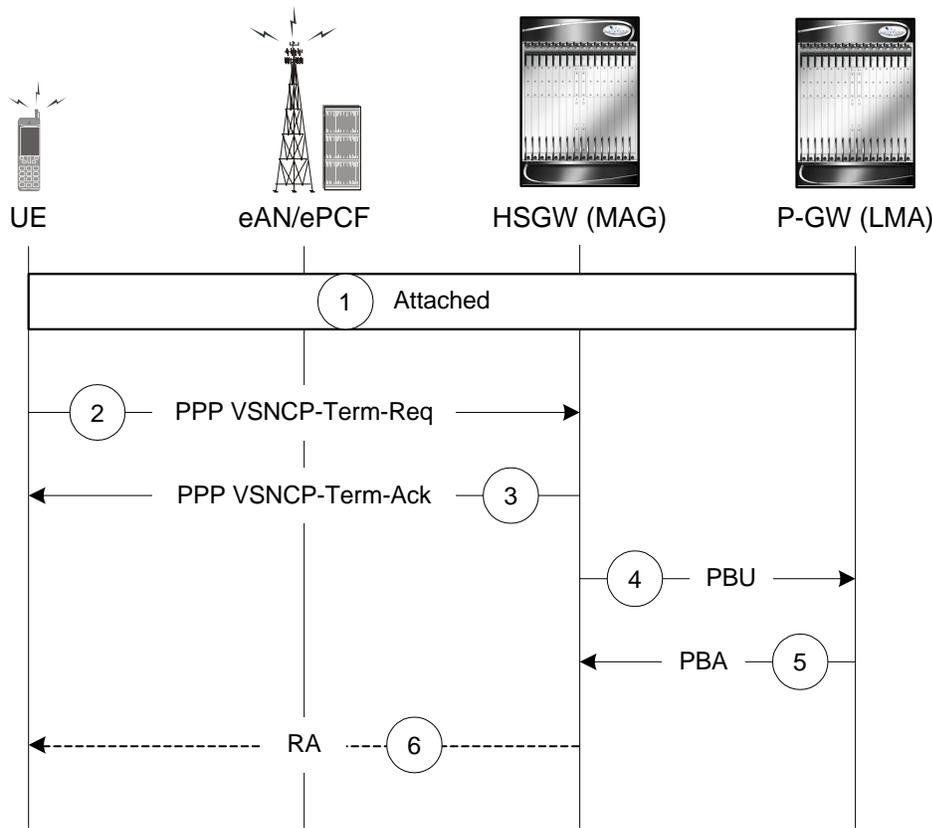


Table 4. PDN Connection Release by the UE Call Flow Description

Step	Description
1	The UE is attached to the EPC and has a PDN connection with the P-GW for PDN-ID=x and APN with assigned HNP.
2	The UE decides to disconnect from the PDN and sends a PPP VSNCP-Term-Req with PDNID=x.
3	The HSGW starts disconnecting the PDN connection and sends a PPP-VSNCP-Term-Ack to the UE (also with PDNID=x).
4	The HSGW begins the tear down of the PMIP session by sending a PBU Deregistration to the P-GW with the following attributes: Lifetime=0, MNID, APN, ATT=HRPD, HNP. The PBU Deregistration message should contain all the mobility options that were present in the initial PBU that created the binding.
5	The P-GW looks up the Binding Cache Entry (BCE) based on the HNP, deletes the binding, and responds to the HSGW with a Deregistration PBA with the same attributes (Lifetime=0, MNID, APN, ATT=HRPD, HNP).
6	The HSGW optionally sends a Router Advertisement (RA) with assigned HNP and prefix lifetime=0.

## PDN Connection Release Initiated by HSGW

This section describes the procedure of a session release by the HSGW.

Figure 12. PDN Connection Release by the HSGW Call Flow

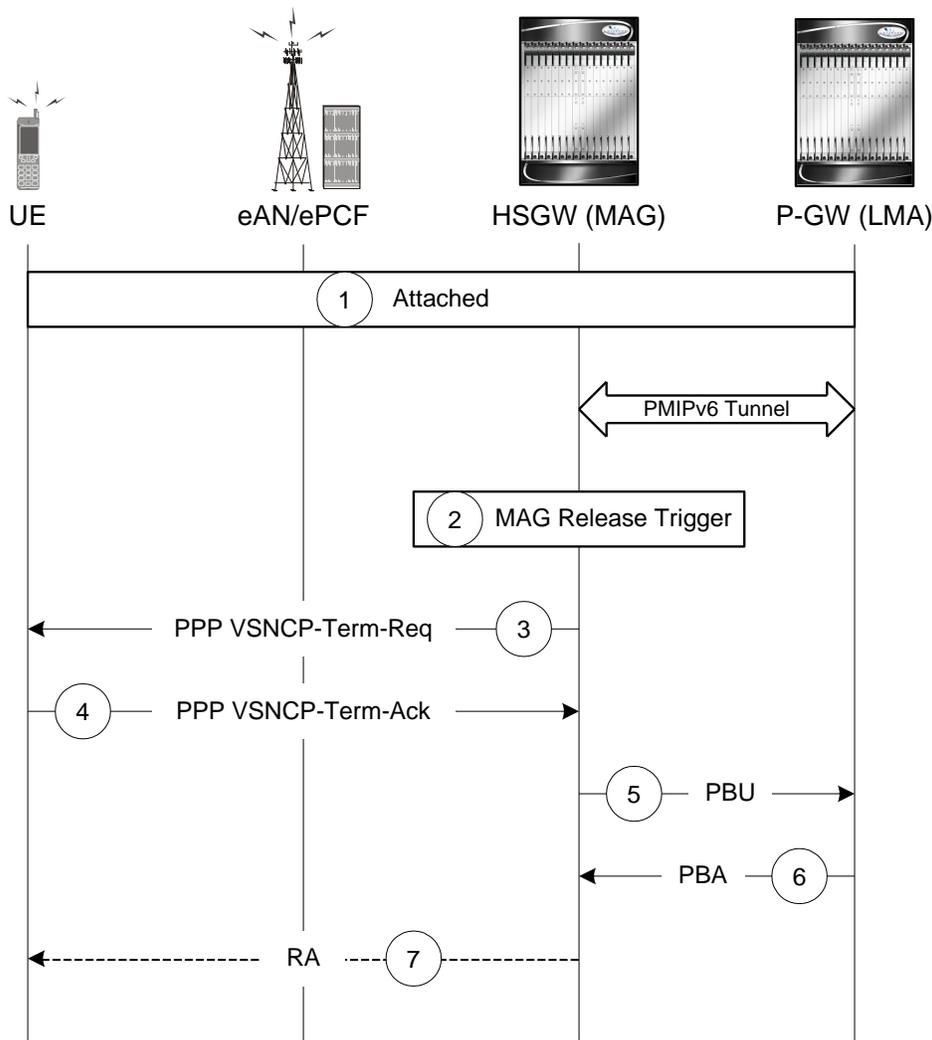


Table 5. PDN Connection Release by the HSGW Call Flow Description

Step	Description
1	The UE is attached to the EPC and has a PDN connection with the P-GW for PDN-ID=x and APN with assigned HNP.
2	The HSGW MAG service triggers a disconnect of the PDN connection for PDNID=x.
3	The HSGW sends a PPP VSNCP-Term-Req with PDNID=x to the UE.
4	The UE acknowledges the receipt of the request with a VSNCP-Term-Ack (PDNID=x).
5	The HSGW begins the tear down of the PMIP session by sending a PBU Deregistration to the P-GW with the following attributes: Lifetime=0, MNID, APN, HNP. The PBU Deregistration message should contain all the mobility options that were present in the initial PBU that created the binding.
6	The P-GW looks up the BCE based on the HNP, deletes the binding, and responds to the HSGW with a Deregistration PBA with the same attributes (Lifetime=0, MNID, APN, ATT=HRPD, HNP).

Step	Description
7	The HSGW optionally sends a Router Advertisement (RA) with assigned HNP and prefix lifetime=0.

### PDN Connection Release Initiated by P-GW

This section describes the procedure of a session release by the P-GW.

Figure 13. PDN Connection Release by the P-GW Call Flow

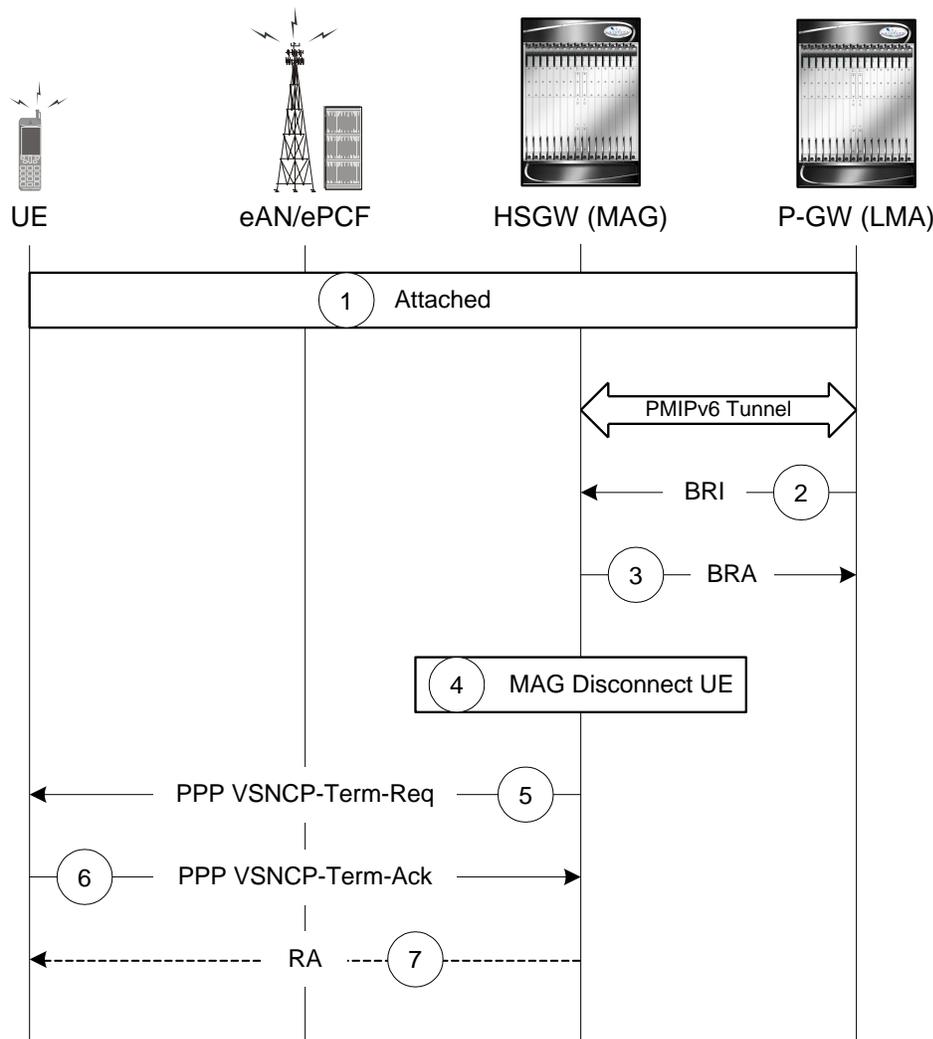


Table 6. PDN Connection Release by the P-GW Call Flow Description

Step	Description
1	The UE is attached to the EPC and has a PDN connection with the P-GW for PDN-ID=x and APN with assigned HNP.

Step	Description
2	A PGW trigger causes a disconnect of the PDN connection for PDNID=x and the PGW sends a Binding Revocation Indication (BRI) message to the HSGW with the following attributes: MNID, APN, HNP.
3	The HSGW responds to the BRI message with a Binding Revocation Acknowledgement (BRA) message with the sane attributes (MNID, APN, HNP).
4	The HSGW MAG service triggers a disconnect of the UE PDN connection for PDNID=x.
5	The HSGW sends a PPP VSNCP-Term-Req with PDNID=x to the UE.
6	The UE acknowledges the receipt of the request with a VSNCP-Term-Ack (PDNID=x).
7	The HSGW optionally sends a Router Advertisement (RA) with assigned HNP and prefix lifetime=0.

## GTP PDN Gateway Call/Session Procedures in an LTE-SAE Network

The following topics and procedure flows are included:

- [Subscriber-initiated Attach \(initial\)](#)
- [Subscriber-initiated Detach](#)

### Subscriber-initiated Attach (initial)

This section describes the procedure of an initial attach to the EPC network by a subscriber.

Figure 14. Subscriber-initiated Attach (initial) Call Flow

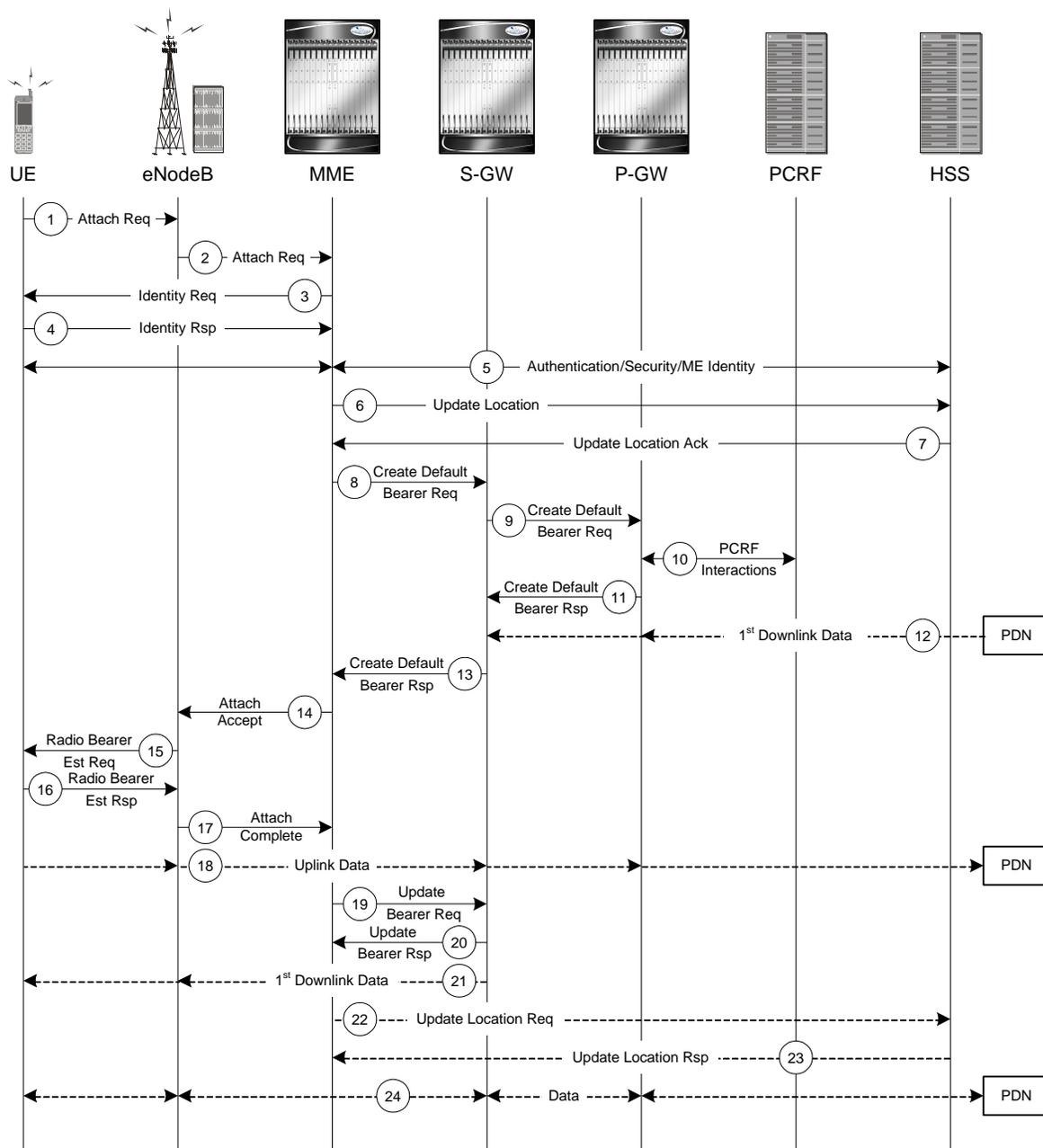


Table 7. Subscriber-initiated Attach (initial) Call Flow Description

Step	Description
1	The UE initiates the Attach procedure by the transmission of an Attach Request (IMSI or old GUTI, last visited TAI (if available), UE Network Capability, PDN Address Allocation, Protocol Configuration Options, Attach Type) message together with an indication of the Selected Network to the eNodeB. IMSI is included if the UE does not have a valid GUTI available. If the UE has a valid GUTI, it is included.

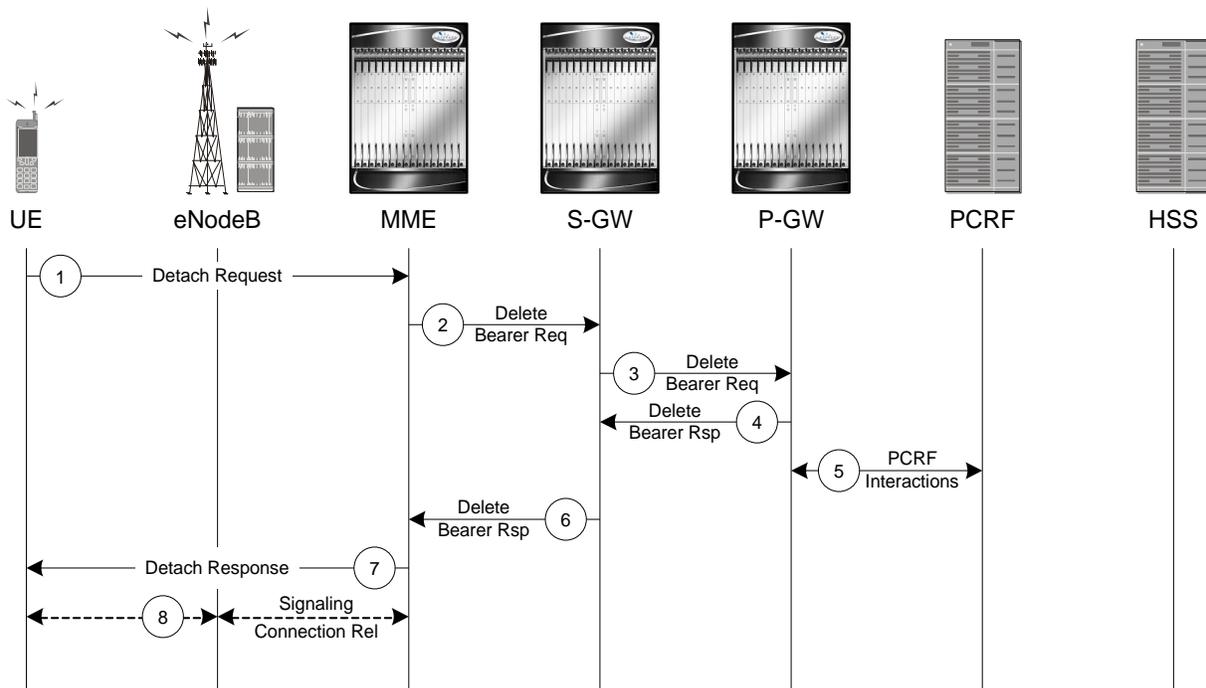
Step	Description
2	The eNodeB derives the MME from the GUTI and from the indicated Selected Network. If that MME is not associated with the eNodeB, the eNodeB selects an MME using an “MME selection function”. The eNodeB forwards the Attach Request message to the new MME contained in a S1-MME control message (Initial UE message) together with the Selected Network and an indication of the E-UTRAN Area identity, a globally unique E-UTRAN ID of the cell from where it received the message to the new MME.
3	If the UE is unknown in the MME, the MME sends an Identity Request to the UE to request the IMSI.
4	The UE responds with Identity Response (IMSI).
5	If no UE context for the UE exists anywhere in the network, authentication is mandatory. Otherwise this step is optional. However, at least integrity checking is started and the ME Identity is retrieved from the UE at Initial Attach. The authentication functions, if performed this step, involves AKA authentication and establishment of a NAS level security association with the UE in order to protect further NAS protocol messages.
6	The MME sends an Update Location (MME Identity, IMSI, ME Identity) to the HSS.
7	The HSS acknowledges the Update Location message by sending an Update Location Ack to the MME. This message also contains the Insert Subscriber Data (IMSI, Subscription Data) Request. The Subscription Data contains the list of all APNs that the UE is permitted to access, an indication about which of those APNs is the Default APN, and the 'EPS subscribed QoS profile' for each permitted APN. If the Update Location is rejected by the HSS, the MME rejects the Attach Request from the UE with an appropriate cause.
8	The MME selects an S-GW using “Serving GW selection function” and allocates an EPS Bearer Identity for the Default Bearer associated with the UE. If the PDN subscription context contains no P-GW address the MME selects a P-GW as described in clause “PDN GW selection function”. Then it sends a Create Default Bearer Request (IMSI, MME Context ID, APN, RAT type, Default Bearer QoS, PDN Address Allocation, AMBR, EPS Bearer Identity, Protocol Configuration Options, ME Identity, User Location Information) message to the selected S-GW.
9	The S-GW creates a new entry in its EPS Bearer table and sends a Create Default Bearer Request (IMSI, APN, S-GW Address for the user plane, S-GW TEID of the user plane, S-GW TEID of the control plane, RAT type, Default Bearer QoS, PDN Address Allocation, AMBR, EPS Bearer Identity, Protocol Configuration Options, ME Identity, User Location Information) message to the P-GW.
10	If dynamic PCC is deployed, the P-GW interacts with the PCRF to get the default PCC rules for the UE. The IMSI, UE IP address, User Location Information, RAT type, AMBR are provided to the PCRF by the P-GW if received by the previous message.
11	The P-GW returns a Create Default Bearer Response (P-GW Address for the user plane, P-GW TEID of the user plane, P-GW TEID of the control plane, PDN Address Information, EPS Bearer Identity, Protocol Configuration Options) message to the S-GW. PDN Address Information is included if the P-GW allocated a PDN address Based on PDN Address Allocation received in the Create Default Bearer Request. PDN Address Information contains an IPv4 address for IPv4 and/or an IPv6 prefix and an Interface Identifier for IPv6. The P-GW takes into account the UE IP version capability indicated in the PDN Address Allocation and the policies of operator when the P-GW allocates the PDN Address Information. Whether the IP address is negotiated by the UE after completion of the Attach procedure, this is indicated in the Create Default Bearer Response.
12	The Downlink (DL) Data can start flowing towards S-GW. The S-GW buffers the data.
13	The S-GW returns a Create Default Bearer Response (PDN Address Information, S-GW address for User Plane, S-GW TEID for User Plane, S-GW Context ID, EPS Bearer Identity, Protocol Configuration Options) message to the new MME. PDN Address Information is included if it was provided by the P-GW.
14	The new MME sends an Attach Accept (APN, GUTI, PDN Address Information, TAI List, EPS Bearer Identity, Session Management Configuration IE, Protocol Configuration Options) message to the eNodeB.
15	The eNodeB sends Radio Bearer Establishment Request including the EPS Radio Bearer Identity to the UE. The Attach Accept message is also sent along to the UE.

Step	Description
16	The UE sends the Radio Bearer Establishment Response to the eNodeB. In this message, the Attach Complete message (EPS Bearer Identity) is included.
17	The eNodeB forwards the Attach Complete (EPS Bearer Identity) message to the MME.
18	The Attach is complete and UE sends data over the default bearer. At this time the UE can send uplink packets towards the eNodeB which are then tunnelled to the S-GW and P-GW.
19	The MME sends an Update Bearer Request (eNodeB address, eNodeB TEID) message to the S-GW.
20	The S-GW acknowledges by sending Update Bearer Response (EPS Bearer Identity) message to the MME.
21	The S-GW sends its buffered downlink packets.
22	After the MME receives Update Bearer Response (EPS Bearer Identity) message, if an EPS bearer was established and the subscription data indicates that the user is allowed to perform handover to non-3GPP accesses, and if the MME selected a P-GW that is different from the P-GW address which was indicated by the HSS in the PDN subscription context, the MME sends an Update Location Request including the APN and P-GW address to the HSS for mobility with non-3GPP accesses.
23	The HSS stores the APN and P-GW address pair and sends an Update Location Response to the MME.
24	Bidirectional data is passed between the UE and PDN.

### Subscriber-initiated Detach

This section describes the procedure of detachment from the EPC network by a subscriber.

Figure 15. Subscriber-initiated Detach Call Flow



**Table 8. Subscriber-initiated Detach Call Flow Description**

Step	Description
1	The UE sends NAS message Detach Request (GUTI, Switch Off) to the MME. Switch Off indicates whether detach is due to a switch off situation or not.
2	The active EPS Bearers in the S-GW regarding this particular UE are deactivated by the MME sending a Delete Bearer Request (TEID) message to the S-GW.
3	The S-GW sends a Delete Bearer Request (TEID) message to the P-GW.
4	The P-GW acknowledges with a Delete Bearer Response (TEID) message.
5	The P-GW may interact with the PCRF to indicate to the PCRF that EPS Bearer is released if PCRF is applied in the network.
6	The S-GW acknowledges with a Delete Bearer Response (TEID) message.
7	If Switch Off indicates that the detach is not due to a switch off situation, the MME sends a Detach Accept message to the UE.
8	The MME releases the S1-MME signalling connection for the UE by sending an S1 Release command to the eNodeB with Cause = Detach.

## Supported Standards

The P-GW service complies with the following standards.

- [Release 9 3GPP References](#)
- [Release 8 3GPP References](#)
- [3GPP2 References](#)
- [IETF References](#)
- [Object Management Group \(OMG\) Standards](#)

## Release 9 3GPP References

---

 **Important:** The P-GW currently supports the following Release 9 3GPP specifications. Most 3GPP specifications are also used for 3GPP2 support; any specifications that are unique to 3GPP2 are listed under *3GPP2 References*.

---

- 3GPP TR 21.905: Vocabulary for 3GPP Specifications
- 3GPP TS 22.115: Service aspects; Charging and billing
- 3GPP TS 23.003: Numbering, addressing and identification
- 3GPP TS 23.007: Restoration procedures
- 3GPP TS 23.060: General Packet Radio Service (GPRS); Service description; Stage 2
- 3GPP TS 23.203: Policy and charging control architecture
- 3GPP TS 23.207: End-to-end Quality of Service (QoS) concept and architecture
- 3GPP TS 23.216: Single Radio Voice Call Continuity (SRVCC); Stage 2
- 3GPP TS 23.228: IP Multimedia Subsystem (IMS); Stage 2
- 3GPP TS 23.401: General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access
- 3GPP TS 23.402: Architecture enhancements for non-3GPP accesses
- 3GPP TS 24.008: Mobile radio interface Layer 3 specification; Core network protocols
- 3GPP TS 29.060: General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface
- 3GPP TS 29.061: Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN)
- 3GPP TS 29.212: Policy and Charging Control over Gx reference point
- 3GPP TS 29.214: Policy and Charging control over Rx reference point
- 3GPP TS 29.229: Cx and Dx interfaces based on Diameter protocol
- 3GPP TS 29.230: Diameter applications; 3GPP specific codes and identifiers
- 3GPP TS 29.272: Evolved Packet System (EPS); Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol

- 3GPP TS 29.273: 3GPP EPS AAA Interfaces
- 3GPP TS 29.274: 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3
- 3GPP TS 29.275: Proxy Mobile IPv6 (PMIPv6) based Mobility and Tunnelling protocols; Stage 3
- 3GPP TS 29.281: General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U)
- 3GPP TS 29.282: Mobile IPv6 vendor specific option format and usage within 3GPP
- 3GPP TS 32.240: Telecommunication management; Charging management; Charging architecture and principles
- 3GPP TS 32.251: Telecommunication management; Charging management; Packet Switched (PS) domain charging
- 3GPP TS 32.298: Telecommunication management; Charging management; Charging Data Record (CDR) parameter description
- 3GPP TS 32.299: Telecommunication management; Charging management; Diameter charging application

## Release 8 3GPP References



**Important:** The P-GW currently supports the following Release 8 3GPP specifications. Most 3GPP specifications are also used for 3GPP2 support; any specifications that are unique to 3GPP2 are listed under *3GPP2 References*.

- 3GPP TR 21.905: Vocabulary for 3GPP Specifications
- 3GPP TS 23.003: Numbering, addressing and identification
- 3GPP TS 23.007: Restoration procedures
- 3GPP TS 23.060: General Packet Radio Service (GPRS); Service description; Stage 2
- 3GPP TS 23.107: Quality of Service (QoS) concept and architecture
- 3GPP TS 23.203: Policy and charging control architecture
- 3GPP TS 23.401: General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access
- 3GPP TS 23.402: Architecture enhancements for non-3GPP accesses
- 3GPP TS 23.869: Support for Internet Protocol (IP) based IP Multimedia Subsystem (IMS) Emergency calls over General Packet Radio Service (GPRS) and Evolved Packet Service (EPS)
- 3GPP TS 24.008: Mobile radio interface Layer 3 specification; Core network protocols
- 3GPP TS 24.229: IP Multimedia Call Control Protocol based on SIP and SDP; Stage 3
- 3GPP TS 27.060: Mobile Station (MS) 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)
- 3GPP TS 29.210: Charging rule provisioning over Gx interface
- 3GPP TS 29.212: Policy and Charging Control over Gx reference point
- 3GPP TS 29.213: Policy and Charging Control signaling flows and QoS
- 3GPP TS 29.273: 3GPP EPS AAA Interfaces

- 3GPP TS 29.274: Evolved GPRS Tunnelling Protocol for Control plane (GTPv2-C)
- 3GPP TS 29.275: Proxy Mobile IPv6 (PMIPv6) based Mobility and Tunnelling protocols
- 3GPP TS 29.281: GPRS Tunnelling Protocol User Plane (GTPv1-U)
- 3GPP TS 29.282: Mobile IPv6 vendor specific option format and usage within 3GPP
- 3GPP TS 32.295: Charging management; Charging Data Record (CDR) transfer
- 3GPP TS 32.298: Telecommunication management; Charging management; Charging Data Record (CDR) encoding rules description
- 3GPP TS 32.299: Charging management; Diameter charging applications
- 3GPP TS 36.300. EUTRA and EUTRAN; Overall description Stage 2
- 3GPP TS 36.412. EUTRAN S1 signaling transport
- 3GPP TS 36.413. EUTRAN S1 Application Protocol (S1AP)

## 3GPP2 References

- X.S0057-0 v3.0 E-UTRAN - eHRPD Connectivity and Interworking: Core Network Aspects

## IETF References

- RFC 768: User Datagram Protocol (STD 6).
- RFC 791: Internet Protocol (STD 5).
- RFC 1701, Generic Routing Encapsulation (GRE)
- RFC 1702, Generic Routing Encapsulation over IPv4 networks
- RFC 2131: Dynamic Host Configuration Protocol
- RFC 2460: Internet Protocol, Version 6 (IPv6) Specification
- RFC 2473: Generic Packet Tunneling in IPv6 Specification
- RFC 2698: A Two Rate Three Color Marker
- RFC 2784: Generic Routing Encapsulation (GRE)
- RFC 2890: Key and Sequence Number Extensions to GRE
- RFC 3162: RADIUS and IPv6
- RFC 3266: Support for IPv6 in Session Description Protocol (SDP)
- RFC 3319: Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers
- RFC 3588: Diameter Base Protocol
- RFC 3589: Diameter Command Codes for Third Generation Partnership Project (3GPP) Release 5
- RFC 3646: DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
- RFC 3775: Mobility Support in IPv6
- RFC 4004: Diameter Mobile IPv4 Application
- RFC 4005: Diameter Network Access Server Application

- RFC 4006: Diameter Credit-Control Application
- RFC 4282: The Network Access Identifier
- RFC 4283: Mobile Node Identifier Option for Mobile IPv6 (MIPv6)
- RFC 4861: Neighbor Discovery for IP Version 6 (IPv6)
- RFC 4862: IPv6 Stateless Address Autoconfiguration
- RFC 5094: Mobile IPv6 Vendor Specific Option
- RFC 5149: Service Selection for Mobile IPv6
- RFC 5213: Proxy Mobile IPv6
- RFC 5447: Diameter Mobile IPv6: Support for NAS to Diameter Server Interaction
- RFC 5555: Mobile IPv6 Support for Dual Stack Hosts and Routers
- RFC 5844: IPv4 Support for Proxy Mobile IPv6
- RFC 5845: Generic Routing Encapsulation (GRE) Key Option for Proxy Mobile IPv6
- RFC 5846: Binding Revocation for IPv6 Mobility
- Internet-Draft (draft-ietf-dime-qos-attributes-07): QoS Attributes for Diameter
- Internet-Draft (draft-ietf-mip6-nemo-v4traversal-06.txt): Mobile IPv6 support for dual stack Hosts and Routers (DSMIPv6)
- Internet-Draft (draft-ietf-netlmm-grekey-option-01.txt): GRE Key Option for Proxy Mobile IPv6, work in progress
- Internet-Draft (draft-ietf-netlmm-pmip6-ipv4-support-02.txt) IPv4 Support for Proxy Mobile IPv6
- Internet-Draft (draft-ietf-netlmm-proxymip6-07.txt): Proxy Mobile IPv6
- Internet-Draft (draft-ietf-mext-binding-revocation-02.txt): Binding Revocation for IPv6 Mobility, work in progress
- Internet-Draft (draft-meghana-netlmm-pmip6-mipv4-00.txt) Proxy Mobile IPv6 and Mobile IPv4 interworking

## Object Management Group (OMG) Standards

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



# Chapter 2

## PDN Gateway Configuration

---

This chapter provides configuration information for the PDN Gateway (P-GW).



**Important:** Information about all commands in this chapter can be found in the *Command Line Interface Reference*.

---

Because each wireless network is unique, the system is designed with a variety of parameters allowing it to perform in various wireless network environments. In this chapter, only the minimum set of parameters are provided to make the system operational. Optional configuration commands specific to the P-GW product are located in the *Command Line Interface Reference*.

The following procedures are located in this chapter:

- [Configuring the System as a Standalone eGTP P-GW](#)
- [Configuring the System as a Standalone PMIP P-GW Supporting an eHRPD Network](#)
- [Configuring Optional Features on the P-GW](#)

# Configuring the System as a Standalone eGTP P-GW

This section provides a high-level series of steps and the associated configuration file examples for configuring the system to perform as a eGTP P-GW in a test environment. For a complete configuration file example, refer to the *Sample Configuration Files* appendix. Information provided in this section includes the following:

- [Information Required](#)
- [How This Configuration Works](#)
- [eGTP P-GW Configuration](#)

## Information Required

The following sections describe the minimum amount of information required to configure and make the P-GW 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 P-GW in the network. Information on these parameters can be found in the appropriate sections of the *Command Line Interface Reference*.

## Required Local Context Configuration Information

The following table lists the information that is required to configure the local context on an P-GW.

Table 9. Required Information for Local Context Configuration

Required Information	Description
Management Interface Configuration	
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	IPv4 addresses assigned to the interface. Multiple addresses and 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 followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the management interface(s) to a specific network.
Security administrator name	The name or names of the security administrator with full rights to the system.
Security administrator password	Open or encrypted passwords can be used.

Required Information	Description
Remote access type(s)	The type of remote access that will be used to access the system such as telnetd, sshd, and/or ftpd.

## Required P-GW Context Configuration Information

The following table lists the information that is required to configure the P-GW context on a P-GW.

**Table 10. Required Information for P-GW Context Configuration**

Required Information	Description
P-GW context name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the P-GW context will be recognized by the system.
Accounting policy name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the accounting policy will be recognized by the system. The accounting policy is used to set parameters for the Rf (off-line charging) interface.
<b>S5/S8 Interface Configuration (To/from S-GW)</b>	
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	IPv4 or IPv6 addresses assigned to the interface. Multiple addresses and 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 followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.
<b>GTP-U Service Configuration</b>	
GTP-U service name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the GTP-U service will be recognized by the system.
IP address	S5/S8 interface IPv4 address.
<b>P-GW Service Configuration</b>	
P-GW service name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the P-GW service will be recognized by the system. Multiple names are needed if multiple P-GW services will be used.
PLMN ID	MCC number: The mobile country code (MCC) portion of the PLMN's identifier (an integer value between 100 and 999). MNC number: The mobile network code (MNC) portion of the PLMN's identifier (a 2 or 3 digit integer value between 00 and 999).

Required Information	Description
eGTP Service Configuration	
eGTP Service Name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the eGTP service will be recognized by the system.

## Required PDN Context Configuration Information

The following table lists the information that is required to configure the PDN context on a P-GW.

Table 11. Required Information for PDN Context Configuration

Required Information	Description
PDN context name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the PDN context is recognized by the system.
IP Address Pool Configuration	
IPv4 address pool name and range	An identification string between 1 and 31 characters (alpha and/or numeric) by which the IPv4 pool is recognized by the system. Multiple names are needed if multiple pools will be configured. A range of IPv4 addresses defined by a starting address and an ending address.
IPv6 address pool name and range	An identification string between 1 and 31 characters (alpha and/or numeric) by which the IPv6 pool is recognized by the system. Multiple names are needed if multiple pools will be configured. A range of IPv6 addresses defined by a starting address and an ending address.
Access Control List Configuration	
IPv4 access list name	An identification string between 1 and 47 characters (alpha and/or numeric) by which the IPv4 access list is recognized by the system. Multiple names are needed if multiple lists will be configured.
IPv6 access list name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the IPv6 access list is recognized by the system. Multiple names are needed if multiple lists will be configured.
Deny/permit type	The types are: <ul style="list-style-type: none"> <li>• any</li> <li>• by host IP address</li> <li>• by IP packets</li> <li>• by source ICMP packets</li> <li>• by source IP address masking</li> <li>• by TCP/UDP packets</li> </ul>

Required Information	Description
Readdress or redirect type	The types are <ul style="list-style-type: none"> <li>• readdress server</li> <li>• redirect context</li> <li>• redirect css delivery-sequence</li> <li>• redirect css service</li> <li>• redirect nexthop</li> </ul>
<b>SGi Interface Configuration (To/from IPv4 PDN)</b>	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv4 addresses assigned to the interface. Multiple addresses and 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 followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.
<b>SGi Interface Configuration (To/from IPv6 PDN)</b>	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv6 addresses assigned to the interface. Multiple addresses and 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 followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.

## Required AAA Context Configuration Information

The following table lists the information that is required to configure the AAA context on a P-GW.

**Table 12. Required Information for AAA Context Configuration**

Required Information	Description
<b>Gx Interface Configuration (to PCRF)</b>	

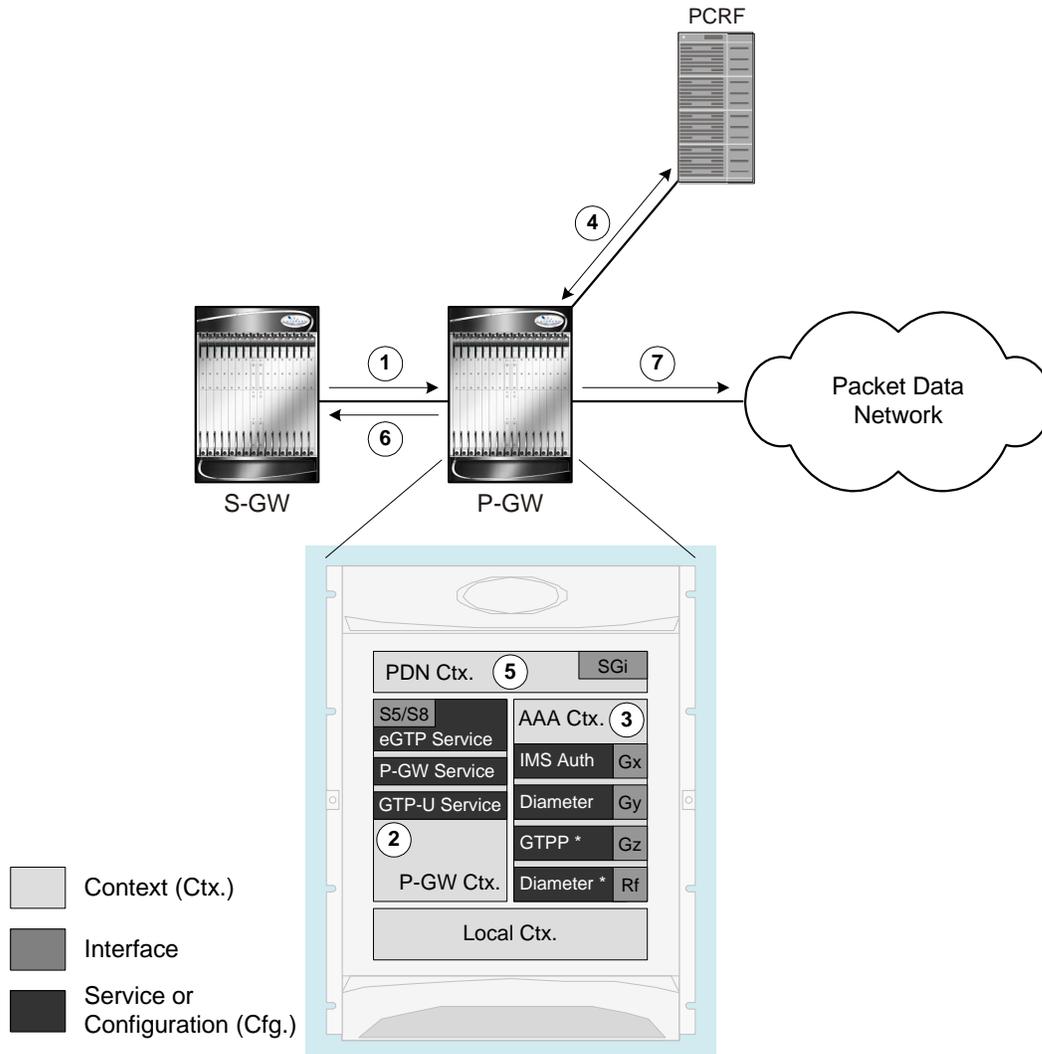
Required Information	Description
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv4 or IPv6 addresses assigned to the interface. Multiple addresses and 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 followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.
<b>Gx Diameter Endpoint Configuration</b>	
End point name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the Gx Diameter endpoint configuration is recognized by the system.
Origin realm name	An identification string between 1 through 127 characters. The realm is the Diameter identity. The originator's realm is present in all Diameter messages and is typically the company or service name.
Origin host name	An identification string from 1 to 255 characters (alpha and/or numeric) by which the Gx origin host is recognized by the system.
Origin host address	The IP address of the Gx interface.
Peer name	The Gx endpoint name described above.
Peer realm name	The Gx origin realm name described above.
Peer address and port number	The IP address and port number of the PCRF.
Route-entry peer	The Gx endpoint name described above.
<b>Gy Interface Configuration (to on-line charging server)</b>	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv4 or IPv6 addresses assigned to the interface. Multiple addresses and 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 followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.
<b>Gy Diameter Endpoint Configuration</b>	

Required Information	Description
End point name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the Gy Diameter endpoint configuration is recognized by the system.
Origin realm name	An identification string between 1 through 127 characters. The realm is the Diameter identity. The originator's realm is present in all Diameter messages and is typically the company or service name.
Origin host name	An identification string from 1 to 255 characters (alpha and/or numeric) by which the Gy origin host is recognized by the system.
Origin host address	The IP address of the Gy interface.
Peer name	The Gy endpoint name described above.
Peer realm name	The Gy origin realm name described above.
Peer address and port number	The IP address and port number of the OCS.
Route-entry peer	The Gy endpoint name described above.
<b>Gz Interface Configuration (to off-line charging server)</b>	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv4 addresses assigned to the interface. Multiple addresses and 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 followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.
<b>Rf Interface Configuration (to off-line charging server)</b>	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv4 or IPv6 addresses assigned to the interface. Multiple addresses and 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 followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.
<b>Rf Diameter Endpoint Configuration</b>	

Required Information	Description
End point name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the Rf Diameter endpoint configuration is recognized by the system.
Origin realm name	An identification string between 1 through 127 characters. The realm is the Diameter identity. The originator's realm is present in all Diameter messages and is typically the company or service name.
Origin host name	An identification string from 1 to 255 characters (alpha and/or numeric) by which the Rf origin host is recognized by the system.
Origin host address	The IP address of the Rf interface.
Peer name	The Rf endpoint name described above.
Peer realm name	The Rf origin realm name described above.
Peer address and port number	The IP address and port number of the OFCS.
Route-entry peer	The Rf endpoint name described above.

## How This Configuration Works

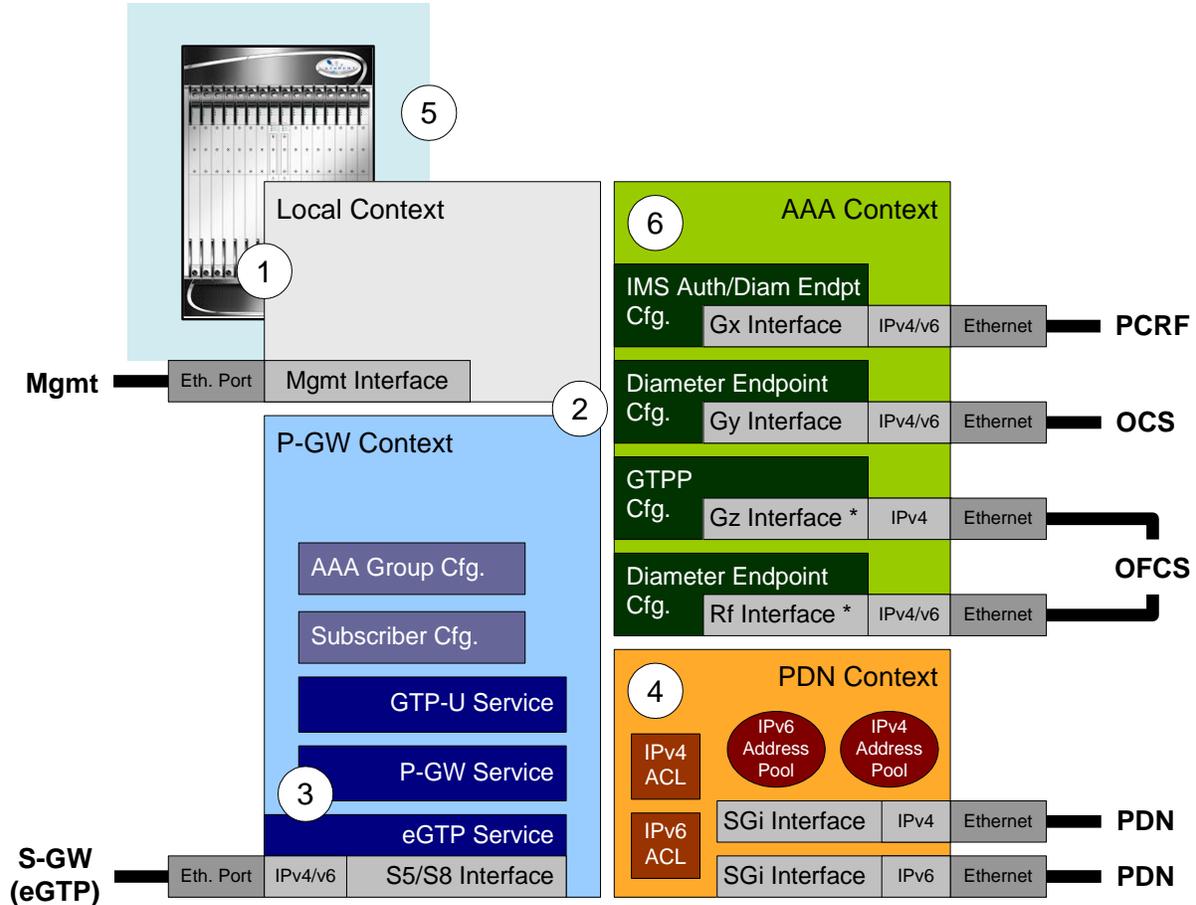
The following figure and supporting text describe how this configuration with a single source and destination context is used by the system to process a subscriber call originating from the GTP LTE network.



1. The S-GW establishes the S5/S8 connection by sending a Create Session Request message to the P-GW including an Access Point name (APN).
2. The P-GW 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*.
3. The P-GW uses the configured Gx Diameter endpoint to establish the IP-CAN session.
4. The P-GW sends a CC-Request (CCR) message to the PCRF to indicate the establishment of the IP-CAN session and the PCRF acknowledges with a CC-Answer (CCA).
5. The P-GW uses the APN configuration to select the PDN context. IP addresses are assigned from the IP pool configured in the selected PDN context.
6. The P-GW responds to the S-GW with a Create Session Response message including the assigned address and additional information.
7. The S5/S8 data plane tunnel is established and the P-GW can forward and receive packets to/from the PDN.

# eGTP P-GW Configuration

To configure the system to perform as a standalone eGTP P-GW:



- Step 1** Set system configuration parameters such as activating PSCs by applying the example configurations found in the *System Administration Guide*.
- Step 2** Set initial configuration parameters such as creating contexts and services by applying the example configurations found in the [Initial Configuration](#) section of this chapter.
- Step 3** Configure the system to perform as an eGTP P-GW and set basic P-GW parameters such as eGTP interfaces and IP routes by applying the example configurations presented in the [P-GW Service Configuration](#) section.
- Step 4** Configure the PDN context by applying the example configuration in the [P-GW PDN Context Configuration](#) section.
- Step 5** Enable and configure the active charging service for Gx interface support by applying the example configuration in the [Active Charging Service Configuration](#) section.
- Step 6** Create a AAA context and configure parameters for policy by applying the example configuration in the [Policy Configuration](#) section.
- Step 7** Verify and save the configuration by following the steps found in the [Verifying and Saving the Configuration](#) section.

## Initial Configuration

- Step 1** Set local system management parameters by applying the example configuration in the [Modifying the Local Context](#) section.
- Step 2** Create the context where the eGTP service will reside by applying the example configuration in the [Creating and Configuring a P-MIP P-GW Context](#) section.
- Step 3** Create and configure APNs in the P-GW context by applying the example configuration in the [Creating and Configuring APNs in the P-GW Context](#) section.
- Step 4** Create and configure AAA server groups in the P-GW context by applying the example configuration in the [Creating and Configuring AAA Groups in the P-GW Context](#) section.
- Step 5** Create an eGTP service within the newly created context by applying the example configuration in the [Creating and Configuring an eGTP Service](#) section.
- Step 6** Create and configure a GTP-U service within the P-GW context by applying the example configuration in the [Creating and Configuring a GTP-U Service](#) section.
- Step 7** Create a context through which the interface to the PDN will reside by applying the example configuration in the [Creating a P-GW PDN Context](#) section.

## Modifying the Local Context

Use the following example to set the default subscriber and configure remote access capability in the local context:

```
configure
  context local
    interface <lcl_cntxt_intrfc_name>
      ip address <ip_address> <ip_mask>
    exit
  server ftpd
    exit
  server telnetd
    exit
  subscriber default
    exit
  administrator <name> encrypted password <password> ftp
  ip route <ip_addr/ip_mask> <next_hop_addr> <lcl_cntxt_intrfc_name>
  exit
```

```

port ethernet <slot#/port#>

no shutdown

bind interface <lcl_cntxt_intrfc_name> local

end

```

## Creating and Configuring an eGTP P-GW Context

Use the following example to create a P-GW context, create an S5/S8 IPv4 interface (for data traffic to/from the S-GW), and bind the S5/S8 interface to a configured Ethernet port:

```

configure

gtp single-source

context <pgw_context_name> -noconfirm

interface <s5s8_interface_name>

ip address <ipv4_address>

exit

gtp group default

gtp charging-agent address <gz_ipv4_address>

gtp echo-interval <seconds>

gtp attribute diagnostics

gtp attribute local-record-sequence-number

gtp attribute node-id-suffix <string>

gtp dictionary <name>

gtp server <ipv4_address> priority <num>

gtp server <ipv4_address> priority <num> node-alive enable

exit

policy accounting <rf_policy_name> -noconfirm

accounting-level {level_type}

accounting-event-trigger interim-timeout action stop-start

operator-string <string>

cc profile <index> interval <seconds>

exit

```

```

    exit

subscriber default

    exit

port ethernet <slot_number/port_number>

    no shutdown

    bind interface <s5s8_interface_name> <pgw_context_name>

end

```

## Notes:

- **gtp single-source** is enabled to allow the system to generate requests to the accounting server using a single UDP port (by way of a AAA proxy function) rather than each AAA manager generating requests on unique UDP ports.
- The S5/S8 (P-GW to S-GW) interface IP address can also be specified as an IPv6 address using the **ipv6 address** command.
- Set the accounting policy for the Rf (off-line charging) interface. The accounting level types are: flow, PDN, PDN-QCI, QCI, and subscriber. Refer to the *Accounting Profile Configuration Mode Commands* chapter in the *Command Line Interface Reference* for more information on this command.
- Set the GTPP group setting for Gz accounting.

## Creating and Configuring APNs in the P-GW Context

Use the following configuration to create an APN:

```

configure

context <pgw_context_name> -noconfirm

    apn <name>

        accounting-mode radius-diameter

        associate accounting-policy <rf_policy_name>

        ims-auth-service <gx_ims_service_name>

        aaa group <rf-radius_group_name>

        dns primary <ipv4_address>

        dns secondary <ipv4_address>

        ip access-group <name> in

        ip access-group <name> out

        mediation-device context-name <pgw_context_name>

        ip context-name <pdn_context_name>

```

```

ipv6 access-group <name> in

ipv6 access-group <name> out

active-charging rulebase <name>

end

```

## Notes:

- The IMS Authorization Service is created and configured in the AAA context.
- Multiple APNs can be configured to support different domain names.
- The associate accounting-policy command is used to associate a pre-configured accounting policy with this APN. Accounting policies are configured in the P-GW context. An example is located in the [Creating and Configuring an eGTP P-GW Context](#) section above.

Use the following configuration to create an APN that includes Gz interface parameters:

```

configure

context <pgw_context_name> -noconfirm

  apn <name>

    bearer-control-mode mixed

    selection-mode sent-by-ms

    accounting-mode gtp

    gtp group default accounting-context <aaa_context_name>

    ims-auth-service <gx_ims_service_name>

    ip access-group <name> in

    ip access-group <name> out

    ip context-name <pdn_context_name>

    active-charging rulebase <gz_rulebase_name>

  end

```

## Notes:

- The IMS Authorization Service is created and configured in the AAA context.
- Multiple APNs can be configured to support different domain names.
- The accounting-mode gtp and gtp group commands configure this APN for Gz accounting.

## Creating and Configuring AAA Groups in the P-GW Context

Use the following example to create and configure AAA groups supporting RADIUS and Rf accounting:

```

configure

```

```
context <pgw_context_name> -noconfirm
  aaa group <rf-radius_group_name>
    radius attribute nas-identifier <id>
    radius accounting interim interval <seconds>
    radius dictionary <name>
    radius mediation-device accounting server <address> key <key>
    diameter authentication dictionary <name>
    diameter accounting dictionary <name>
    diameter accounting endpoint <rf_cfg_name>
    diameter accounting server <rf_cfg_name> priority <num>
  exit
aaa group default
  radius attribute nas-ip-address address <ipv4_address>
  radius accounting interim interval <seconds>
  diameter authentication dictionary <name>
  diameter accounting dictionary <name>
  diameter accounting endpoint <rf_cfg_name>
  diameter accounting server <rf_cfg_name> priority <num>
```

## Creating and Configuring an eGTP Service

Use the following configuration example to create the eGTP service:

```
configure
  context <pgw_context_name>
    egtp-service <egtp_service_name> -noconfirm
      interface-type interface-pgw-ingress
      validation mode default
      associate gtpu-service <gtpu_service_name>
      gtpc bind address <s5s8_interface_address>
    end
```

Notes:

- Co-locating a GGSN service on the same ASR 5x00 requires that the `gtpc bind address` command uses the same IP address the GGSN service is bound to.

## Creating and Configuring a GTP-U Service

Use the following configuration example to create the GTP-U service:

```
configure
  context <pgw_context_name>
    gtpu-service <gtpu_service_name> -noconfirm
    bind ipv4-address <s5s8_interface_address>
  end
```

Notes:

- The `bind` command can also be specified as an IPv6 address using the `ipv6-address` command.

## Creating a P-GW PDN Context

Use the following example to create a P-GW PDN context and Ethernet interface, and bind the interface to a configured Ethernet port.

```
configure
  context <pdn_context_name> -noconfirm
    interface <sgi_ipv4_interface_name>
      ip address <ipv4_address>
    interface <sgi_ipv6_interface_name>
      ipv6 address <address>
  end
```

## P-GW Service Configuration

- Step 1** Configure the P-GW service by applying the example configuration in the [Configuring the P-GW Service](#) section.
- Step 2** Specify an IP route to the eGTP Serving Gateway by applying the example configuration in the [Configuring a Static IP Route](#) section.

## Configuring the P-GW Service

Use the following example to configure the P-GW service:

```
configure
```

```

context <pgw_context_name>

  pgw-service <pgw_service_name> -noconfirm

    plmn id mcc <id> mnc <id>

    associate egtp-service <egtp_service_name>

    associate qci-qos-mapping <name>

  end

```

**Notes:**

- QCI-QoS mapping configurations are created in the AAA context. Refer to the [Configuring QCI-QoS Mapping](#) section for more information.
- Co-locating a GGSN service on the same ASR 5x00 requires the configuration of the **associate ggsn-service** *name* command within the P-GW service.

## Configuring a Static IP Route

Use the following example to configure an IP Route for control and user plane data communication with an eGTP Serving Gateway:

```

configure

  context <pgw_context_name>

    ip route <sgw_ip_addr/mask> <sgw_next_hop_addr> <pgw_intrfc_name>

  end

```

## P-GW PDN Context Configuration

Use the following example to configure an IP Pool and APN, and bind a port to the interface in the PDN context:

```

configure

  context <pdn_context_name> -noconfirm

    interface <sgi_ipv4_interface_name>

      ip address <ipv4_address>

    exit

    interface <sgi_ipv6_interface_name>

      ip address <ipv6_address>

    exit

    ip pool <name> range <start_address end_address> public <priority>

    ipv6 pool <name> range <start_address end_address> public <priority>

```

```
subscriber default
    exit

ip access-list <name>
    redirect css service <name> any
    permit any
    exit

ipv6 access-list <name>
    redirect css service <name> any
    permit any
    exit

aaa group default
    exit

exit

port ethernet <slot_number/port_number>
    no shutdown
    bind interface <sgi_ipv4_interface_name> <pdn_context_name>
    exit

port ethernet <slot_number/port_number>
    no shutdown
    bind interface <sgi_ipv6_interface_name> <pdn_context_name>
    exit

end
```

## Active Charging Service Configuration

Use the following example to enable and configure active charging:

```
configure
    require active-charging optimized-mode
    active-charging service <name>
        ruledef <name>
            <rule_definition>
```

```

        .
        .
    <rule_definition>
    exit
ruledef default
    ip any-match = TRUE
    exit
ruledef icmp-pkts
    icmp any-match = TRUE
    exit
ruledef qci3
    icmp any-match = TRUE
    exit
ruledef static
    icmp any-match = TRUE
    exit
charging-action <name>
    <action>
        .
        .
    <action>
    exit
charging-action icmp
    billing-action egcdr
    exit
charging-action qci3
    content-id <id>
    billing-action egcdr
    qos-class-identifier <id>

```

```
allocation-retention-priority <priority>
tft-packet-filter qci3
exit
charging-action static
service-identifier <id>
billing-action egcdr
qos-class-identifier <id>
allocation-retention-priority <priority>
tft-packet-filter qci3
exit
rulebase default
exit
rulebase <name>
<rule_base>
.
.
<rule_base>
exit
rulebase <gx_rulebase_name>
dynamic-rule order first-if-tied
egcdr tariff minute <minute> hour <hour> (optional)
billing-records egcdr
action priority 5 dynamic-only ruledef qci3 charging-action qci3
action priority 100 ruledef static charging-action static
action priority 500 ruledef default charging-action icmp
action priority 570 ruledef icmp-pkts charging-action icmp
egcdr threshold interval <interval>
egcdr threshold volume total <bytes>
end
```

## Notes:

- A rule base is a collection of rule definitions and associated charging actions.
- As depicted above, multiple rule definitions, charging actions, and rule bases can be configured to support a variety of charging scenarios.
- Charging actions define the action to take when a rule definition is matched.
- Routing and/or charging rule definitions can be created/configured. The maximum number of routing rule definitions that can be created is 256. The maximum number of charging rule definitions is 2048.
- The billing-action `egcdr` command in the charging-action `qc13`, `icmp`, and `static` examples is required for Gz accounting.
- The Gz rulebase example supports the Gz interface for off-line charging. The `billing-records egcdr` command is required for Gz accounting. All other commands are optional.

## Policy Configuration

- Step 1** Configure the policy and accounting interfaces by applying the example configuration in the [Creating and Configuring the AAA Context](#) section.
- Step 2** Create and configure QCI to QoS mapping by applying the example configuration in the [Configuring QCI-QoS Mapping](#) section.

## Creating and Configuring the AAA Context

Use the following example to create and configure a AAA context including diameter support and policy control, and bind Ethernet ports to interfaces supporting traffic between this context and a PCRF, an OCS, and an OFCS:

```
configure

context <aaa_context_name> -noconfirm

    interface <gx_interface_name>

        ipv6 address <address>

        exit

    interface <gy_interface_name>

        ipv6 address <address>

        exit

    interface <gz_interface_name>

        ip address <ipv4_address>

        exit

    interface <rf_interface_name>

        ip address <ipv4_address>
```

```

    exit

subscriber default

    exit

ims-auth-service <gx_ims_service_name>

    p-cscf discovery table <#> algorithm round-robin

    p-cscf table <#> row-precedence <#> ipv6-address <pcrf_ipv6_adr>

    policy-control

        diameter origin endpoint <gx_cfg_name>

        diameter dictionary <name>

        diameter host-select table <#> algorithm round-robin

        diameter host-select row-precedence <#> table <#> host <gx_cfg_name>

    exit

exit

diameter endpoint <gx_cfg_name>

    origin realm <realm_name>

    origin host <name> address <aaa_ctx_ipv6_address>

    peer <gx_cfg_name> realm <name> address <pcrf_ipv4_or_ipv6_addr>

    route-entry peer <gx_cfg_name>

    exit

diameter endpoint <gy_cfg_name>

    origin realm <realm_name>

    origin host <name> address <gy_ipv6_address>

    connection retry-timeout <seconds>

    peer <gy_cfg_name> realm <name> address <ocs_ipv4_or_ipv6_addr>

    route-entry peer <gy_cfg_name>

    exit

diameter endpoint <rf_cfg_name>

    use-proxy

    origin realm <realm_name>

```

```
    origin host <name> address <rf_ipv4_address>

    peer <rf_cfg_name> realm <name> address <ofcs_ipv4_or_ipv6_addr>

    route-entry peer <rf_cfg_name>

    exit

exit

port ethernet <slot_number/port_number>

    no shutdown

    bind interface <gx_interface_name> <aaa_context_name>

    exit

port ethernet <slot_number/port_number>

    no shutdown

    bind interface <gy_interface_name> <aaa_context_name>

    exit

port ethernet <slot_number/port_number>

    no shutdown

    bind interface <gz_interface_name> <aaa_context_name>

    exit

port ethernet <slot_number/port_number>

    no shutdown

    bind interface <rf_interface_name> <aaa_context_name>

    end
```

#### Notes:

- The **p-cscf table** command under **ims-auth-service** can also specify an IPv4 address to the PCRF.
- The Gx interface IP address can also be specified as an IPv4 address using the **ip address** command.
- The Gy interface IP address can also be specified as an IPv4 address using the **ip address** command.
- The Rf interface IP address can also be specified as an IPv6 address using the **ipv6 address** command.

## Configuring QCI-QoS Mapping

Use the following example to create and map QCI values to enforceable QoS parameters:

```
configure
```

```
qci-qos-mapping <name>

  qci 1 user-datagram dscp-marking <hex>

  qci 3 user-datagram dscp-marking <hex>

  qci 9 user-datagram dscp-marking <hex>

  exit
```

Notes:

- QCI values 1 through 9 are standard values and are defined in 3GPP TS 23.203. Values 10 through 32 can be configured for non-standard use.
- The above configuration only shows one keyword example. Refer to the *QCI - QOS Mapping Configuration Mode Commands* chapter in the *Command Line Interface Reference* for more information on the **qci** command and other supported keywords.

## Verifying and Saving the Configuration

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 System as a Standalone PMIP P-GW Supporting an eHRPD Network

This section provides a high-level series of steps and the associated configuration file examples for configuring the system to perform as a P-MIP P-GW supporting an eHRPD test environment. For a complete configuration file example, refer to the *Sample Configuration Files* appendix. Information provided in this section includes the following:

- [Information Required](#)
- [How This Configuration Works](#)
- [P-MIP P-GW \(eHRPD\) Configuration](#)

## Information Required

The following sections describe the minimum amount of information required to configure and make the P-GW 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 P-GW in the network. Information on these parameters can be found in the appropriate sections of the *Command Line Interface Reference*.

## Required Local Context Configuration Information

The following table lists the information that is required to configure the local context on an P-GW.

Table 13. Required Information for Local Context Configuration

Required Information	Description
Management Interface Configuration	
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	IPv4 addresses assigned to the interface. Multiple addresses and 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 followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the management interface(s) to a specific network.
Security administrator name	The name or names of the security administrator with full rights to the system.

Required Information	Description
Security administrator password	Open or encrypted passwords can be used.
Remote access type(s)	The type of remote access that will be used to access the system such as telnetd, sshd, and/or ftpd.

## Required P-GW Context Configuration Information

The following table lists the information that is required to configure the P-GW context on a P-GW.

Table 14. Required Information for P-GW Context Configuration

Required Information	Description
P-GW context name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the P-GW context will be recognized by the system.
Accounting policy name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the accounting policy will be recognized by the system. The accounting policy is used to set parameters for the Rf (off-line charging) interface.
S2a Interface Configuration (To/from HSGW)	
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	IPv6 addresses assigned to the interface. Multiple addresses and 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 followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.
P-GW Service Configuration	
P-GW service name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the P-GW service will be recognized by the system. Multiple names are needed if multiple P-GW services will be used.
PLMN ID	MCC number: The mobile country code (MCC) portion of the PLMN's identifier (an integer value between 100 and 999). MNC number: The mobile network code (MNC) portion of the PLMN's identifier (a 2 or 3 digit integer value between 00 and 999).
LMA Service Configuration	

Required Information	Description
LMA Service Name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the LMA service will be recognized by the system.

## Required PDN Context Configuration Information

The following table lists the information that is required to configure the PDN context on a P-GW.

**Table 15. Required Information for PDN Context Configuration**

Required Information	Description
P-GW context name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the P-GW context is recognized by the system.
IP Address Pool Configuration	
IPv4 address pool name and range	An identification string between 1 and 31 characters (alpha and/or numeric) by which the IPv4 pool is recognized by the system. Multiple names are needed if multiple pools will be configured. A range of IPv4 addresses defined by a starting address and an ending address.
IPv6 address pool name and range	An identification string between 1 and 31 characters (alpha and/or numeric) by which the IPv6 pool is recognized by the system. Multiple names are needed if multiple pools will be configured. A range of IPv6 addresses defined by a starting address and an ending address.
Access Control List Configuration	
IPv4 access list name	An identification string between 1 and 47 characters (alpha and/or numeric) by which the IPv4 access list is recognized by the system. Multiple names are needed if multiple lists will be configured.
IPv6 access list name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the IPv6 access list is recognized by the system. Multiple names are needed if multiple lists will be configured.
Deny/permit type	The types are: <ul style="list-style-type: none"> <li>• any</li> <li>• by host IP address</li> <li>• by IP packets</li> <li>• by source ICMP packets</li> <li>• by source IP address masking</li> <li>• by TCP/UDP packets</li> </ul>

Required Information	Description
Readdress or redirect type	The types are <ul style="list-style-type: none"> <li>• readdress server</li> <li>• redirect context</li> <li>• redirect css delivery-sequence</li> <li>• redirect css service</li> <li>• redirect nexthop</li> </ul>
SGi Interface Configuration (To/from IPv4 PDN)	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv4 addresses assigned to the interface. Multiple addresses and 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 followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.
SGi Interface Configuration (To/from IPv6 PDN)	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv6 addresses assigned to the interface. Multiple addresses and 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 followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.

## Required AAA Context Configuration Information

The following table lists the information that is required to configure the AAA context on a P-GW.

Table 16. Required Information for AAA Context Configuration

Required Information	Description
Gx Interface Configuration (to PCRF)	

Required Information	Description
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv4 or IPv6 addresses assigned to the interface. Multiple addresses and 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 followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.
<b>Gx Diameter Endpoint Configuration</b>	
End point name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the Gx Diameter endpoint configuration is recognized by the system.
Origin realm name	An identification string between 1 through 127 characters. The realm is the Diameter identity. The originator's realm is present in all Diameter messages and is typically the company or service name.
Origin host name	An identification string from 1 to 255 characters (alpha and/or numeric) by which the Gx origin host is recognized by the system.
Origin host address	The IP address of the Gx interface.
Peer name	The Gx endpoint name described above.
Peer realm name	The Gx origin realm name described above.
Peer address and port number	The IP address and port number of the PCRF.
Route-entry peer	The Gx endpoint name described above.
<b>S6b Interface Configuration (to 3GPP AAA server)</b>	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv4 or IPv6 addresses assigned to the interface. Multiple addresses and 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 followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.
<b>S6b Diameter Endpoint Configuration</b>	

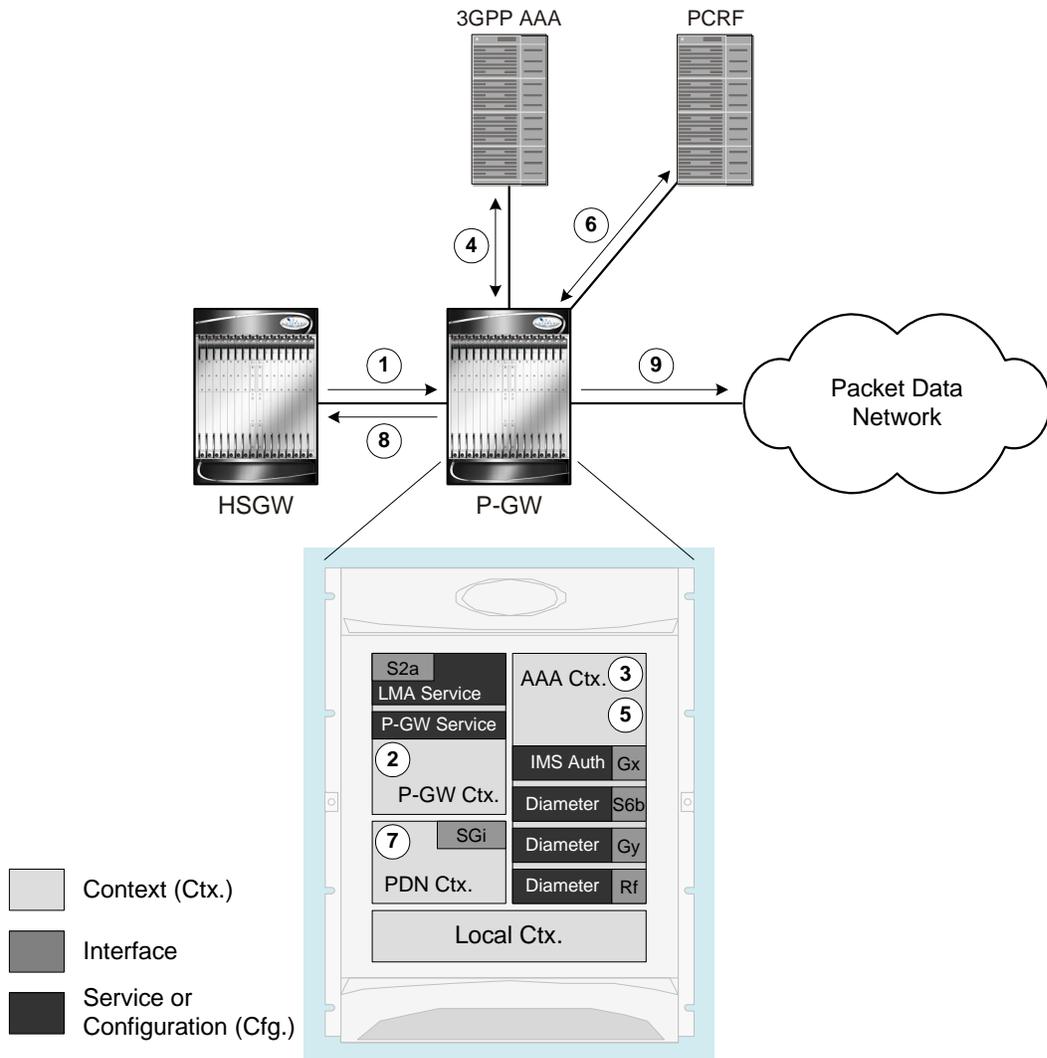
■ Configuring the System as a Standalone PMIP P-GW Supporting an eHRPD Network

Required Information	Description
End point name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the S6b Diameter endpoint configuration is recognized by the system.
Origin realm name	An identification string between 1 through 127 characters. The realm is the Diameter identity. The originator's realm is present in all Diameter messages and is typically the company or service name.
Origin host name	An identification string from 1 to 255 characters (alpha and/or numeric) by which the S6b origin host is recognized by the system.
Origin host address	The IP address of the S6b interface.
Peer name	The S6b endpoint name described above.
Peer realm name	The S6b origin realm name described above.
Peer address and port number	The IP address and port number of the AAA server.
Route-entry peer	The S6b endpoint name described above.
<b>Rf Interface Configuration (to off-line charging server)</b>	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv4 or IPv6 addresses assigned to the interface. Multiple addresses and 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 followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the management interface(s) to a specific network.
<b>Rf Diameter Endpoint Configuration</b>	
End point name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the Rf Diameter endpoint configuration is recognized by the system.
Origin realm name	An identification string between 1 through 127 characters. The realm is the Diameter identity. The originator's realm is present in all Diameter messages and is typically the company or service name.
Origin host name	An identification string from 1 to 255 characters (alpha and/or numeric) by which the Rf origin host is recognized by the system.
Origin host address	The IP address of the Rf interface.
Peer name	The Rf endpoint name described above.
Peer realm name	The Rf origin realm name described above.

Required Information	Description
Peer address and port number	The IP address and port number of the OFCS.
Route-entry peer	The Rf endpoint name described above.
<b>Gy Interface Configuration (to on-line charging server)</b>	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv4 or IPv6 addresses assigned to the interface. Multiple addresses and 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 followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.
<b>Gy Diameter Endpoint Configuration</b>	
End point name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the Gy Diameter endpoint configuration is recognized by the system.
Origin realm name	An identification string between 1 through 127 characters. The realm is the Diameter identity. The originator's realm is present in all Diameter messages and is typically the company or service name.
Origin host name	An identification string from 1 to 255 characters (alpha and/or numeric) by which the Gy origin host is recognized by the system.
Origin host address	The IP address of the Gy interface.
Peer name	The Gy endpoint name described above.
Peer realm name	The Gy origin realm name described above.
Peer address and port number	The IP address and port number of the OCS.
Route-entry peer	The Gy endpoint name described above.

## How This Configuration Works

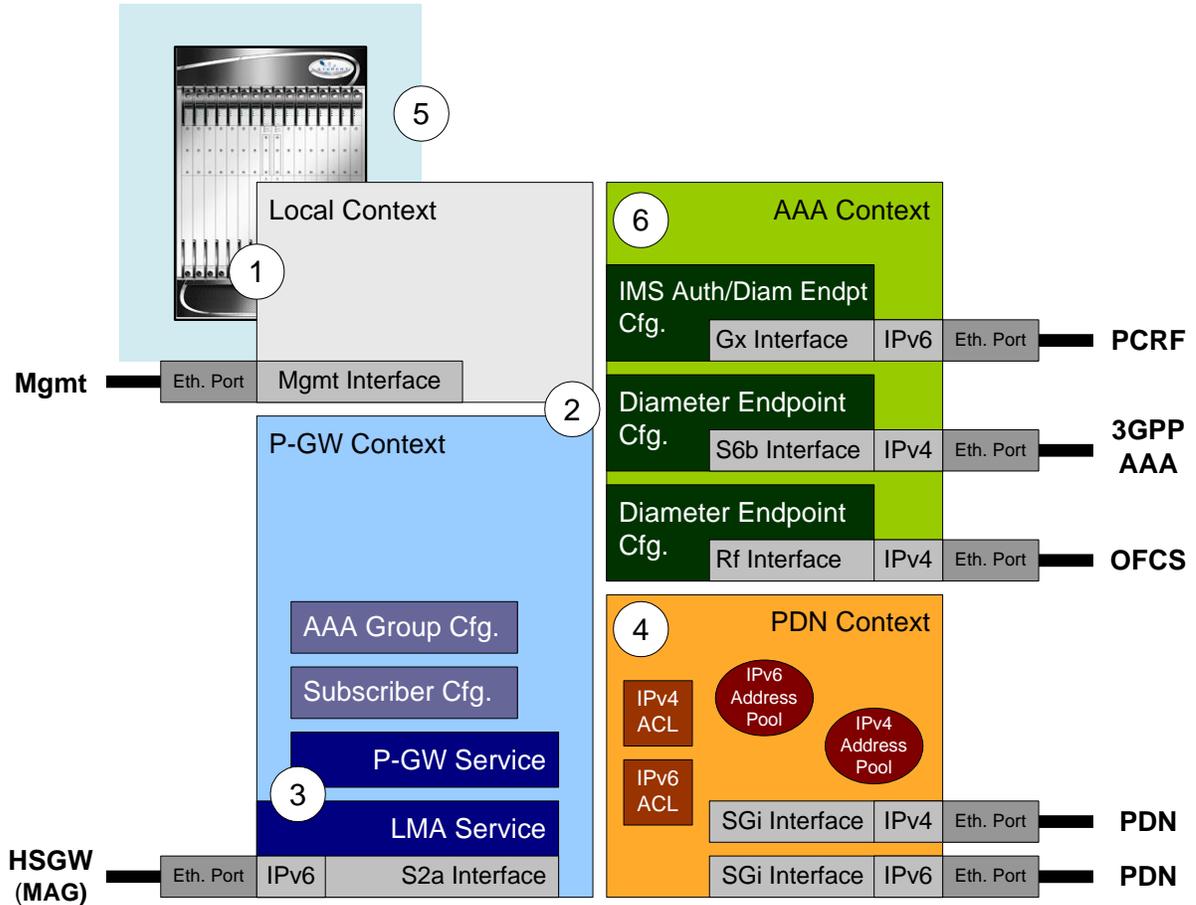
The following figure and supporting text describe how this configuration with a single source and destination context is used by the system to process a subscriber call originating from the GTP LTE network.



1. The S-GW establishes the S5/S8 connection by sending a Create Session Request message to the P-GW including an Access Point name (APN).
2. The P-GW 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*.
3. The P-GW uses the configured Gx Diameter endpoint to establish the IP-CAN session.
4. The P-GW sends a CC-Request (CCR) message to the PCRF to indicate the establishment of the IP-CAN session and the PCRF acknowledges with a CC-Answer (CCA).
5. The P-GW uses the APN configuration to select the PDN context. IP addresses are assigned from the IP pool configured in the selected PDN context.
6. The P-GW responds to the S-GW with a Create Session Response message including the assigned address and additional information.
7. The S5/S8 data plane tunnel is established and the P-GW can forward and receive packets to/from the PDN.

## P-MIP P-GW (eHRPD) Configuration

To configure the system to perform as a standalone P-MIP P-GW in an eHRPD network environment, review the following graphic and subsequent steps.



- Step 1** Set system configuration parameters such as activating PSCs by applying the example configurations found in the *System Administration Guide*.
- Step 2** Set initial configuration parameters such as creating contexts and services by applying the example configurations found in the [Initial Configuration](#) section of this chapter.
- Step 3** Configure the system to perform as a P-MIP P-GW and set basic P-GW parameters such as P-MIP interfaces and an IP route by applying the example configurations presented in the [P-GW Service Configuration](#) section.
- Step 4** Configure the PDN context by applying the example configuration in the [P-GW PDN Context Configuration](#) section.
- Step 5** Enable and configure the active charging service for Gx interface support by applying the example configuration in the [Active Charging Service Configuration](#) section.
- Step 6** Create a AAA context and configure parameters for AAA and policy by applying the example configuration in the [AAA and Policy Configuration](#) section.
- Step 7** Verify and save the configuration by following the instruction in the [Verifying and Saving the Configuration](#) section.

## Initial Configuration

- Step 1** Set local system management parameters by applying the example configuration in the [Modifying the Local Context](#) section.
- Step 2** Create the context where the P-GW service will reside by applying the example configuration in the [Creating and Configuring a P-MIP P-GW Context](#) section.
- Step 3** Create and configure APNs in the P-GW context by applying the example configuration in the [Creating and Configuring APNs in the P-GW Context](#) section.
- Step 4** Create and configure AAA server groups in the P-GW context by applying the example configuration in the [Creating and Configuring AAA Groups in the P-GW Context](#) section.
- Step 5** Create an eGTP service within the newly created context by applying the example configuration in the [Creating and Configuring an LMA Service](#) section.
- Step 6** Create a context through which the interface to the PDN will reside by applying the example configuration in the [Creating a P-GW PDN Context](#) section.

## Modifying the Local Context

Use the following example to set the default subscriber and configure remote access capability in the local context:

```
configure
  context local
    interface <lcl_cntxt_intrfc_name>
      ip address <ip_address> <ip_mask>
    exit
  server ftpd
    exit
  server telnetd
    exit
  subscriber default
    exit
  administrator <name> encrypted password <password> ftp
  ip route <ip_addr/ip_mask> <next_hop_addr> <lcl_cntxt_intrfc_name>
  exit
  port ethernet <slot#/port#>
    no shutdown
```

```
bind interface <lcl_cntxt_intrfc_name> local
end
```

## Creating and Configuring a P-MIP P-GW Context

Use the following example to create a P-GW context, create an S2a IPv6 interface (for data traffic to/from the HSGW), and bind the S2a interface to a configured Ethernet port:

```
configure

context <pgw_context_name> -noconfirm

interface <s2a_interface_name> tunnel

    ipv6 address <address>

    tunnel-mode ipv6ip

        source interface <name>

        destination address <ipv4 or ipv6 address>

    exit

exit

policy accounting <rf_policy_name> -noconfirm

    accounting-level {level_type}

    accounting-event-trigger interim-timeout action stop-start

    operator-string <string>

    cc profile <index> interval <seconds>

    exit

subscriber default

    exit

exit

port ethernet <slot_number/port_number>

    no shutdown

    bind interface <s2a_interface_name> <pgw_context_name>

end
```

### Notes:

- The S2a (P-GW to HSGW) interface must be an IPv6 address.

- Set the accounting policy for the Rf (off-line charging) interface. The accounting level types are: flow, PDN, PDN-QCI, QCI, and subscriber. Refer to the *Accounting Profile Configuration Mode Commands* chapter in the *Command Line Interface Reference* for more information on this command.

## Creating and Configuring APNs in the P-GW Context

Use the following configuration to create an APN:

```
configure

context <pgw_context_name> -noconfirm

  apn <name>

    accounting-mode radius-diameter

    associate accounting-policy <rf_policy_name>

    ims-auth-service <gx_ims_service_name>

    aaa group <rf-radius_group_name>

    dns primary <ipv4_address>

    dns secondary <ipv4_address>

    ip access-group <name> in

    ip access-group <name> out

    mediation-device context-name <pgw_context_name>

    ip context-name <pdn_context_name>

    ipv6 access-group <name> in

    ipv6 access-group <name> out

    active-charging rulebase <name>
```

Notes:

- The IMS Authorization Service is created and configured in the AAA context.
- Multiple APNs can be configured to support different domain names.
- The associate accounting-policy command is used to associate a pre-configured accounting policy with this APN. Accounting policies are configured in the P-GW context. An example is located in the [Creating and Configuring a P-MIP P-GW Context](#) section above.

## Creating and Configuring AAA Groups in the P-GW Context

Use the following example to create and configure AAA groups supporting RADIUS and Rf accounting:

```
configure

context <pgw_context_name> -noconfirm
```

```
aaa group <rf-radius_group_name>
    radius attribute nas-identifier <id>
    radius accounting interim interval <seconds>
    radius dictionary <name>
    radius mediation-device accounting server <address> key <key>
    diameter authentication dictionary <name>
    diameter accounting dictionary <name>
    diameter authentication endpoint <s6b_cfg_name>
    diameter accounting endpoint <rf_cfg_name>
    diameter authentication server <s6b_cfg_name> priority <num>
    diameter accounting server <rf_cfg_name> priority <num>
    exit
aaa group default
    radius attribute nas-ip-address address <ipv4_address>
    radius accounting interim interval <seconds>
    diameter authentication dictionary <name>
    diameter accounting dictionary <name>
    diameter authentication endpoint <s6b_cfg_name>
    diameter accounting endpoint <rf_cfg_name>
    diameter authentication server <s6b_cfg_name> priority <num>
    diameter accounting server <rf_cfg_name> priority <num>
```

## Creating and Configuring an LMA Service

Use the following configuration example to create the LMA service:

```
configure
    context <pgw_context_name>
        lma-service <lma_service_name> -noconfirm
        no aaa accounting
        revocation enable
```

```
bind address <s2a_ipv6_address>
end
```

Notes:

- The **no aaa accounting** command is used to prevent duplicate accounting packets.
- Enabling revocation provides for MIP registration revocation in the event that MIP revocation is negotiated with a MAG and a MIP binding is terminated, the LMA can send a revocation message to the MAG.

## Creating a P-GW PDN Context

Use the following example to create a P-GW PDN context and Ethernet interfaces.

```
configure
context <pdn_context_name> -noconfirm
interface <sgi_ipv4_interface_name>
ip address <ipv4_address>
exit
interface <sgi_ipv6_interface_name>
ipv6 address <address>
end
```

## P-GW Service Configuration

- Step 1** Configure the P-GW service by applying the example configuration in the [Configuring the P-GW Service](#) section.
- Step 2** Specify an IP route to the HRPD Serving Gateway by applying the example configuration in the [Configuring a Static IP Route](#) section.

## Configuring the P-GW Service

Use the following example to configure the P-GW service:

```
configure
context <pgw_context_name>
pgw-service <pgw_service_name> -noconfirm
associate lma-service <lma_service_name>
associate qci-qos-mapping <name>
authorize external
fqdn host <domain_name> realm <realm_name>
```

```

plmn id mcc <id> mnc <id>

end

```

## Notes:

- QCI-QoS mapping configurations are created in the AAA context. Refer to the [Configuring QCI-QoS Mapping](#) section for more information.
- External authorization is performed by the 3GPP AAA server through the S6b interface. Internal authorization (APN) is default.
- The `fqdn host` command configures a Fully Qualified Domain Name for the P-GW service used in messages between the P-GW and a 3GPP AAA server over the S6b interface.

## Configuring a Static IP Route

Use the following example to configure static IP routes for data traffic between the P-GW and the HSGW:

```

configure

context <pgw_context_name>

    ipv6 route <ipv6_addr/prefix> next-hop <hsgw_addr> interface <pgw_hsgw_intrfc_name>

end

```

## Notes:

- Static IP routing is not required for configurations using dynamic routing protocols.

## P-GW PDN Context Configuration

Use the following example to configure IP pools and IP Access Control Lists (ACLs), and bind ports to the interfaces in the PDN context:

```

configure

context <pdn_context_name> -noconfirm

    ip pool <name> range <start_address end_address> public <priority>

    ipv6 pool <name> range <start_address end_address> public <priority>

    subscriber default

    exit

    ip access-list <name>

        redirect css service <name> any

        permit any

    exit

    ipv6 access-list <name>

```

```
        redirect css service <name> any

        permit any

        exit

    aaa group default

        exit

    exit

port ethernet <slot_number/port_number>

    no shutdown

    bind interface <pdn_sgi_ipv4_interface_name> <pdn_context_name>

    exit

port ethernet <slot_number/port_number>

    no shutdown

    bind interface <pdn_sgi_ipv6_interface_name> <pdn_context_name>

    end
```

## Active Charging Service Configuration

Use the following example to enable and configure active charging:

```
configure

    require active-charging optimized-mode

    active-charging service <name>

        ruledef <name>

            <rule_definition>

                .

                .

            <rule_definition>

        exit

    ruledef <name>

        <rule_definition>

            .
```

```

        .
    <rule_definition>
    exit
charging-action <name>
    <action>
        .
        .
    <action>
    exit
charging-action <name>
    <action>
        .
        .
    <action>
    exit
rulebase default
    exit
rulebase <name>
    <rule_base>
        .
        .
    <rule_base>
end
    
```

Notes:

- Active charging in optimized mode enables the service as part of the session manager instead of part of ACS managers.
- As depicted above, multiple rule definitions, charging actions, and rule bases can be configured to support a variety of charging scenarios.
- Routing and/or charging rule definitions can be created/configured. The maximum number of routing rule definitions that can be created is 256. The maximum number of charging rule definitions is 2048.
- Charging actions define the action to take when a rule definition is matched.

- A rule base is a collection of rule definitions and associated charging actions.

## AAA and Policy Configuration

- Step 1** Configure AAA and policy interfaces by applying the example configuration in the [Creating and Configuring the AAA Context](#) section.
- Step 2** Create and configure QCI to QoS mapping by applying the example configuration in the [Configuring QCI-QoS Mapping](#) section.

### Creating and Configuring the AAA Context

Use the following example to create and configure a AAA context including diameter support and policy control, and bind ports to interfaces supporting traffic between this context, a PCRF, a 3GPP AAA server, an on-line charging server, and an off-line charging server:

```
configure

context <aaa_context_name> -noconfirm

    interface <s6b_interface_name>

        ip address <ipv4_address>

        exit

    interface <gx_interface_name>

        ipv6 address <address>

        exit

    interface <rf_interface_name>

        ip address <ipv4_address>

        exit

    interface <gy_interface_name>

        ipv6 address <address>

        exit

    subscriber default

        exit

    ims-auth-service <gx_ims_service_name>

        p-cscf discovery table <#> algorithm round-robin

        p-cscf table <#> row-precedence <#> ipv6-address <pcrf_adr>

    policy-control
```

```

diameter origin endpoint <gx_cfg_name>

diameter dictionary <name>

diameter host-select table <#> algorithm round-robin

diameter host-select row-precedence <#> table <#> host <gx_cfg_name>

exit

exit

diameter endpoint <s6b_cfg_name>

origin realm <realm_name>

origin host <name> address <aaa_ctx_ipv4_address>

peer <s6b_cfg_name> realm <name> address <aaa_ip_addr>

route-entry peer <s6b_cfg_name>

exit

diameter endpoint <gx_cfg_name>

origin realm <realm_name>

origin host <name> address <aaa_context_ip_address>

peer <gx_cfg_name> realm <name> address <pcrf_ipv6_addr>

route-entry peer <gx_cfg_name>

exit

diameter endpoint <rf_cfg_name>

origin realm <realm_name>

origin host <name> address <aaa_ip_address>

peer <rf_cfg_name> realm <name> address <ofcs_ip_addr>

route-entry peer <rf_cfg_name>

exit

diameter endpoint <gy_cfg_name>

use-proxy

origin realm <realm_name>

origin host <name> address <aaa_ip_address>

connection retry-timeout <seconds>

```

```

    peer <gy_cfg_name> realm <name> address <ocs_ip_addr>

    route-entry peer <gy_cfg_name>

    exit

exit

port ethernet <slot_number/port_number>

    no shutdown

    bind interface <s6b_interface_name> <aaa_context_name>

    exit

port ethernet <slot_number/port_number>

    no shutdown

    bind interface <gx_interface_name> <aaa_context_name>

    exit

port ethernet <slot_number/port_number>

    no shutdown

    bind interface <gy_interface_name> <aaa_context_name>

    exit

port ethernet <slot_number/port_number>

    no shutdown

    bind interface <rf_interface_name> <aaa_context_name>

    end

```

**Notes:**

- The **p-cscf table** command under **ims-auth-service** can also specify an IPv4 address to the PCRF.
- The S6b interface IP address can also be specified as an IPv6 address using the **ipv6 address** command.
- The Gx interface IP address can also be specified as an IPv4 address using the **ip address** command.
- The Gy interface IP address can also be specified as an IPv4 address using the **ip address** command.
- The Rf interface IP address can also be specified as an IPv6 address using the **ipv6 address** command.

**Configuring QCI-QoS Mapping**

Use the following example to create and map QCI values to enforceable QoS parameters:

```

configure

    qci-qos-mapping <name>

```

```
qci 1 user-datagram dscp-marking <hex>
qci 3 user-datagram dscp-marking <hex>
qci 9 user-datagram dscp-marking <hex>
exit
```

Notes:

- QCI values 1 through 9 are standard values and are defined in 3GPP TS 23.203. Values 10 through 32 can be configured for non-standard use.
- The above configuration only shows one keyword example. Refer to the *QCI - QoS Mapping Configuration Mode Commands* chapter in the *Command Line Interface Reference* for more information on the `qci` command and other supported keywords.

## Verifying and Saving the Configuration

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 Optional Features on the P-GW

The configuration examples in this section are optional and provided to cover the most common uses of the P-GW in a live network. The intent of these examples is to provide a base configuration for testing.

The following optional configurations are provided in this section:

- [Configuring ACL-based Node-to-Node IP Security on the S5 Interface](#)
- [Configuring APN as Emergency](#)
- [Configuring Dynamic Node-to-Node IP Security on the S5 Interface](#)
- [Configuring Local QoS Policy](#)
- [Configuring X.509 Certificate-based Peer Authentication](#)

### Configuring ACL-based Node-to-Node IP Security on the S5 Interface

The configuration example in this section creates an IKEv2/IPSec ACL-based node-to-node tunnel endpoint on the S5 interface.

---

 **Important:** Use of the IP Security feature requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

---

The following configuration examples are included in this section:

- [Creating and Configuring a Crypto Access Control List](#)
- [Creating and Configuring an IPSec Transform Set](#)
- [Creating and Configuring an IKEv2 Transform Set](#)
- [Creating and Configuring a Crypto Map](#)

### Creating and Configuring a Crypto Access Control List

The following example configures a crypto ACL (Access Control List), which defines the matching criteria used for routing subscriber data packets over an IPSec tunnel:

```
configure
  context <pgw_context_name> -noconfirm
    ip access-list <acl_name>
      permit tcp host <source_host_address> host <dest_host_address>
    end
```

Notes:

- The **permit** command in this example routes IPv4 traffic from the server with the specified source host IPv4 address to the server with the specified destination host IPv4 address.

## Creating and Configuring an IPSec Transform Set

The following example configures an IPSec transform set, which is used to define the security association that determines the protocols used to protect the data on the interface:

```
configure
context <pgw_context_name> -noconfirm
    ipsec transform-set <ipsec_transform-set_name>
        encryption aes-cbc-128
        group none
        hmac sha1-96
        mode tunnel
    end
```

Notes:

- The encryption algorithm, **aes-cbc-128**, or Advanced Encryption Standard Cipher Block Chaining, is the default algorithm for IPSec transform sets configured on the system.
- The **group none** command specifies that no crypto strength is included and that Perfect Forward Secrecy is disabled. This is the default setting for IPSec transform sets configured on the system.
- The **hmac** command configures the Encapsulating Security Payload (ESP) integrity algorithm. The **sha1-96** keyword uses a 160-bit secret key to produce a 160-bit authenticator value. This is the default setting for IPSec transform sets configured on the system.
- The **mode tunnel** command specifies that the entire packet is to be encapsulated by the IPSec header including the IP header. This is the default setting for IPSec transform sets configured on the system.

## Creating and Configuring an IKEv2 Transform Set

The following example configures an IKEv2 transform set:

```
configure
context <pgw_context_name> -noconfirm
    ikev2-ikesa transform-set <ikev2_transform-set_name>
        encryption aes-cbc-128
        group 2
```

```

    hmac sha1-96

    lifetime <sec>

    prf sha1

    end

```

## Notes:

- The encryption algorithm, **aes-cbc-128**, or Advanced Encryption Standard Cipher Block Chaining, is the default algorithm for IKEv2 transform sets configured on the system.
- The **group 2** command specifies the Diffie-Hellman algorithm as Group 2, indicating medium security. The Diffie-Hellman algorithm controls the strength of the crypto exponentials. This is the default setting for IKEv2 transform sets configured on the system.
- The **hmac** command configures the Encapsulating Security Payload (ESP) integrity algorithm. The **sha1-96** keyword uses a 160-bit secret key to produce a 160-bit authenticator value. This is the default setting for IKEv2 transform sets configured on the system.
- The **lifetime** command configures the time the security key is allowed to exist, in seconds.
- The **prf** command configures the IKE Pseudo-random Function which produces a string of bits that cannot be distinguished from a random bit string without knowledge of the secret key. The **sha1** keyword uses a 160-bit secret key to produce a 160-bit authenticator value. This is the default setting for IKEv2 transform sets configured on the system.

## Creating and Configuring a Crypto Map

The following example configures an IKEv2 crypto map:

```

configure

context <pgw_context_name>

    crypto map <crypto_map_name> ikev2-ipv4

        match address <acl_name>

        peer <ipv4_address>

        authentication local pre-shared-key key <text>

        authentication remote pre-shared-key key <text>

        ikev2-ikesa transform-set list <name1> . . . name6>

        payload <name> match ipv4

            lifetime <seconds>

            ipsec transform-set list <name1> . . . <name4>

        exit

```

```
    exit

interface <s5_intf_name>

    ip address <ipv4_address>

    crypto-map <crypto_map_name>

    exit

exit

port ethernet <slot_number/port_number>

    no shutdown

    bind interface <s5_intf_name> <pgw_context_name>

end
```

**Notes:**

- The type of crypto map used in this example is IKEv2/IPv4 for IPv4 addressing. An IKEv2/IPv6 crypto map can also be used for IPv6 addressing.
- The `ipsec transform-set list` command specifies up to four IPsec transform sets.

## Configuring APN as Emergency

The configuration example in this section configures an emergency APN for VoLTE based E911 support.

In APN Configuration Mode, specify the name of the emergency APN and set the emergency inactivity timeout as follows. You may also configure the P-CSCF FQDN server name for the APN.

```
configure

context <pgw_context_name> -noconfirm

    apn <name>

        emergency-apn

        timeout emergency-inactivity <seconds>

        p-cscf fqdn <fqdn>

    end
```

**Notes:**

- By default, an APN is assumed to be non-emergency.
- The `timeout emergency-inactivity` command specifies the timeout duration, in seconds, to check inactivity on the emergency session. `<seconds>` must be an integer value from 1 through 3600.
- By default, emergency inactivity timeout is disabled (0).

- The `p-cscf fqdn` command configures the P-CSCF FQDN server name for the APN. `<fqdn>` must be a string from 1 to 256 characters in length.
- P-CSCF FQDN has more significance than CLI-configured P-CSCF IPv4 and IPv6 addresses.

## Configuring Dynamic Node-to-Node IP Security on the S5 Interface

The configuration example in this section creates an IPSec/IKEv2 dynamic node-to-node tunnel endpoint on the S5 interface.

---

 **Important:** Use of the IP Security feature requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

---

The following configuration examples are included in this section:

- [Creating and Configuring an IPSec Transform Set](#)
- [Creating and Configuring an IKEv2 Transform Set](#)
- [Creating and Configuring a Crypto Template](#)
- [Binding the S5 IP Address to the Crypto Template](#)

### Creating and Configuring an IPSec Transform Set

The following example configures an IPSec transform set, which is used to define the security association that determines the protocols used to protect the data on the interface:

```
configure
context <pgw_context_name> -noconfirm
    ipsec transform-set <ipsec_transform-set_name>
        encryption aes-cbc-128
        group none
        hmac sha1-96
        mode tunnel
    end
```

Notes:

- The encryption algorithm, `aes-cbc-128`, or Advanced Encryption Standard Cipher Block Chaining, is the default algorithm for IPSec transform sets configured on the system.
- The `group none` command specifies that no crypto strength is included and that Perfect Forward Secrecy is disabled. This is the default setting for IPSec transform sets configured on the system.

- The **hmac** command configures the Encapsulating Security Payload (ESP) integrity algorithm. The **sha1-96** keyword uses a 160-bit secret key to produce a 160-bit authenticator value. This is the default setting for IPSec transform sets configured on the system.
- The **mode tunnel** command specifies that the entire packet is to be encapsulated by the IPSec header, including the IP header. This is the default setting for IPSec transform sets configured on the system.

## Creating and Configuring an IKEv2 Transform Set

The following example configures an IKEv2 transform set:

```
configure

context <pgw_context_name> -noconfirm

    ikev2-ikesa transform-set <ikev2_transform-set_name>

        encryption aes-cbc-128

        group 2

        hmac sha1-96

        lifetime <sec>

        prf sha1

    end
```

Notes:

- The encryption algorithm, **aes-cbc-128**, or Advanced Encryption Standard Cipher Block Chaining, is the default algorithm for IKEv2 transform sets configured on the system.
- The **group 2** command specifies the Diffie-Hellman algorithm as Group 2, indicating medium security. The Diffie-Hellman algorithm controls the strength of the crypto exponentials. This is the default setting for IKEv2 transform sets configured on the system.
- The **hmac** command configures the Encapsulating Security Payload (ESP) integrity algorithm. The **sha1-96** keyword uses a 160-bit secret key to produce a 160-bit authenticator value. This is the default setting for IKEv2 transform sets configured on the system.
- The **lifetime** command configures the time the security key is allowed to exist, in seconds.
- The **prf** command configures the IKE Pseudo-random Function, which produces a string of bits that cannot be distinguished from a random bit string without knowledge of the secret key. The **sha1** keyword uses a 160-bit secret key to produce a 160-bit authenticator value. This is the default setting for IKEv2 transform sets configured on the system.

## Creating and Configuring a Crypto Template

The following example configures an IKEv2 crypto template:

```

configure
  context <pgw_context_name> -noconfirm
    crypto template <crypto_template_name> ikev2-dynamic
      ikev2-ikesa transform-set list <name1> . . . <name6>
      ikev2-ikesa rekey
      payload <name> match childsa match ipv4
      ipsec transform-set list <name1> . . . <name4>
      rekey
    end

```

## Notes:

- The **ikev2-ikesa transform-set list** command specifies up to six IKEv2 transform sets.
- The **ipsec transform-set list** command specifies up to four IPsec transform sets.

## Binding the S5 IP Address to the Crypto Template

The following example configures the binding of the S5 interface to the crypto template:

```

configure
  context <pgw_ingress_context_name> -noconfirm
    gtpu-service <gtpu_ingress_service_name>
      bind ipv4-address <s5_interface_ip_address> crypto-template
      <sgw_s5_crypto_template>
      exit
    egtp-service <egtp_ingress_service_name>
      interface-type interface-pgw-ingress
      associate gtpu-service <gtpu_ingress_service_name>
      gtpc bind ipv4-address <s5_interface_ip_address>
      exit
    pgw-service <pgw_service_name> -noconfirm
      plmn id mcc <id> mnc <id> primary
      associate egtp-service <egtp_ingress_service_name>

```

```
end
```

Notes:

- The **bind** command in the GTP-U and eGTP service configuration can also be specified as an IPv6 address using the **ipv6-address** command.

## Configuring Local QoS Policy

The configuration examples in this section create a local QoS policy. A local QoS policy service can be used to control different aspects of a session, such as QoS, data usage, subscription profiles, or server usage, by means of locally defined policies.

---

 **Important:** Local QoS Policy is a licensed feature and requires the purchase of the Local Policy Decision Engine feature license to enable it.

---

The following configuration examples are included in this section:

- [Creating and Configuring a Local QoS Policy](#)
- [Binding a Local QoS Policy](#)
- [Verifying Local QoS Policy](#)

### Creating and Configuring a Local QoS Policy

The following configuration example enables a local QoS policy on the P-GW:

```
configure

local-policy-service <name> -noconfirm

  ruledef <ruledef_name> -noconfirm

    condition priority <priority> <variable> match <string_value>

    condition priority <priority> <variable> match <int_value>

    condition priority <priority> <variable> nomatch <regex>

  exit

  actiondef <actiondef_name> -noconfirm

    action priority <priority> <action_name> <arguments>

    action priority <priority> <action_name> <arguments>

  exit

  actiondef <actiondef_name> -noconfirm

    action priority <priority> <action_name> <arguments>
```

```

    action priority <priority> <action_name> <arguments>

    exit

    eventbase <eventbase_name> -noconfirm

    rule priority <priority> event <list_of_events> ruledef <ruledef_name> actiondef
    <actiondef_name>

    end

```

## Notes:

- A maximum of 16 local QoS policy services are supported.
- A maximum 256 ruledefs are suggested in a local QoS policy service for performance reasons.
- The **condition** command can be entered multiple times to configure multiple conditions for a ruledef. The conditions are examined in priority order until a match is found and the corresponding condition is applied.
- A maximum of 256 actiondefs are suggested in a local QoS policy service for performance reasons.
- The **action** command can be entered multiple times to configure multiple actions for an actiondef. The actions are examined in priority order until a match is found and the corresponding action is applied.
- Currently, only one eventbase is supported and must be named “default”.
- The **rule** command can be entered multiple times to configure multiple rules for an eventbase.
- A maximum of 256 rules are suggested in an eventbase for performance reasons.
- Rules are executed in priority order, and if the rule is matched the action specified in the actiondef is executed. If an event qualifier is associated with a rule, the rule is matched only for that specific event. If a qualifier of **continue** is present at the end of the rule, the subsequent rules are also matched; otherwise, rule evaluation is terminated on first match.

## Binding a Local QoS Policy

The following configuration example binds the previously configured local QoS policy:

```

configure

    context <pgw_context_name> -noconfirm

        apn <name>

            ims-auth-service <local-policy-service name>

        end

```

## Notes:

- A maximum of 16 authorization services can be configured globally in the system. There is also a system limit for the maximum number of total configured services.

## Verifying Local QoS Policy

The following configuration example verifies if local QoS service is enforced:

```
logging filter active facility local-policy level debug
logging active
show local-policy statistics all
```

Notes:

- Please take extreme caution not to use logging feature in console port and in production nodes.

## Configuring X.509 Certificate-based Peer Authentication

The configuration example in this section enables X.509 certificate-based peer authentication, which can be used as the authentication method for IP Security on the P-GW.

---

 **Important:** Use of the IP Security feature requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

---

The following configuration example enables X.509 certificate-based peer authentication on the P-GW. In Global Configuration Mode, specify the name of the X.509 certificate and CA certificate, as follows:

```
configure
    certificate name <cert_name> pem url <cert_pem_url> private-key pem url
    <private_key_url>
    ca-certificate name <ca_cert_name> pem url <ca_cert_url>
end
```

Notes:

- The **certificate name** and **ca-certificate list ca-cert-name** commands specify the X.509 certificate and CA certificate to be used.
- The PEM-formatted data for the certificate and CA certificate can be specified, or the information can be read from a file via a specified URL as shown in this example.

When creating the crypto template for IPSec in Context Configuration Mode, bind the X.509 certificate and CA certificate to the crypto template and enable X.509 certificate-based peer authentication for the local and remote nodes, as follows:

```
configure
    context <pgw_context_name> -noconfirm
        crypto template <crypto_template_name> ikev2-dynamic
            certificate name <cert_name>
```

```
ca-certificate list ca-cert-name <ca_cert_name>

authentication local certificate

authentication remote certificate

end
```

## Notes:

- A maximum of 16 certificates and 16 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.
- The **certificate name** and **ca-certificate list ca-cert-name** commands bind the certificate and CA certificate to the crypto template.
- The **authentication local certificate** and **authentication remote certificate** commands enable X.509 certificate-based peer authentication for the local and remote nodes.

# Chapter 3

## Network Mobility (NEMO)

---

This chapter describes the system's support for NEMO 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 *Cisco ASR 5x00 Packet Data Network Gateway Administration Guide*, before using the procedures in this chapter.

This chapter includes the following sections:

- [NEMO Overview](#)
- [NEMO Configuration](#)

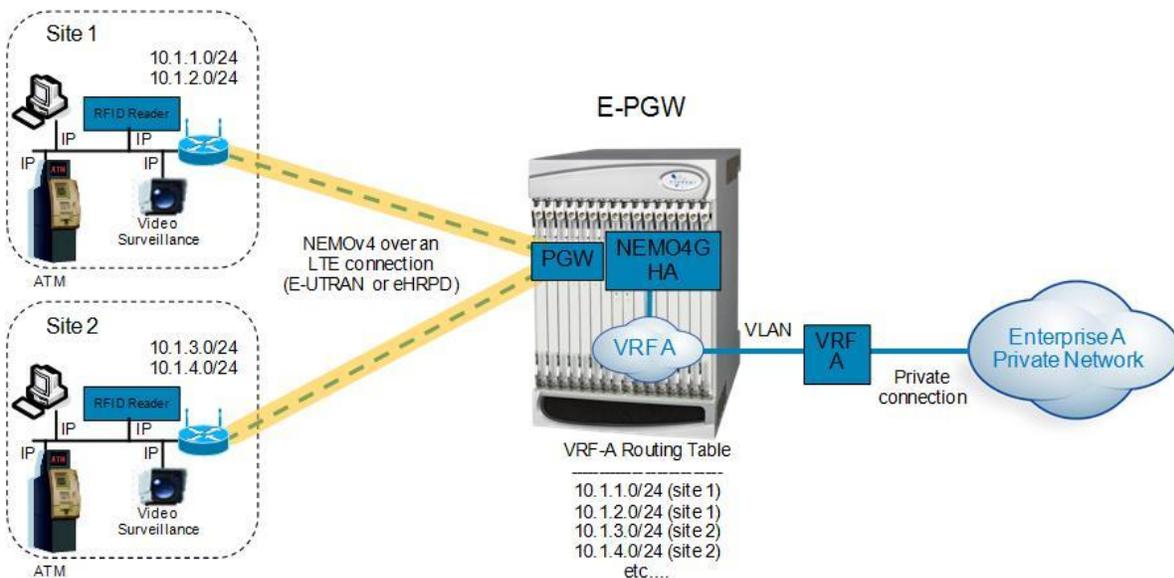
## NEMO Overview

When enabled through a feature license key, the system includes NEMO support for a Mobile IPv4 Network Mobility (NEMO-HA) on the P-GW platform to terminate Mobile IPv4 based NEMO connections from Mobile Routers (MRs) that attach to an Enterprise PDN. The NEMO functionality allows bi-directional communication that is application-agnostic between users behind the MR and users or resources on Fixed Network sites.

The same NEMO4G-HA service and its bound Loopback IP address supports NEMO connections whose underlying PDN connection comes through GTP S5 (4G access) or PMIPv6 S2a (eHRPD access).

The following figure shows a high-level view of LTE NEMOv4 Architecture.

Figure 16. NEMO Overview



## Use Cases

The following use cases are supported by NEMO in LTE:

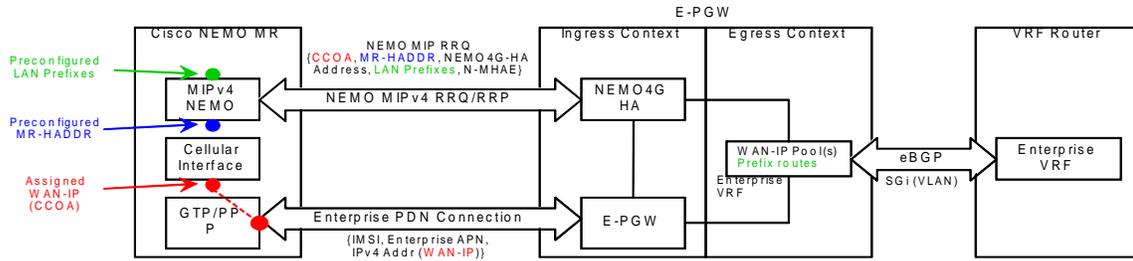
1. **Stationary** - Applications, like branch offices, with a mobile router that does not require mobility.
2. **Nomadic** - Applications that use a mobile router that does not move while in service, but that may be moved to a different location and brought back on service (e.g. a kiosk showing up in a mall one day and in a different location the next day or month).
3. **Moveable** - Applications that need to maintain Dynamic Mobile Network Routing (DMNR) service operational while moving and crossing PDSN boundaries, such as public safety vehicles. Service continuity is handled by the mobility protocols (Mobile IP in 3G and GTP in LTE).

## Features and Benefits

The system supports the usage of dynamically learned, overlapping customer prefixes. These prefixes are advertised via BGP.

### MIPv4-based NEMO Control Plane

The following figure shows a high-level view of the NEMO control plane.



NEMO includes the following features:

- Collocated-Care-of-Address mode

The Cisco NEMO MR is expected to use the Collocated-Care-of-Address mode to establish a NEMO MIPv4 session with NEMO4G-HA and as one of the IP endpoints of the NEMO GRE Tunnel for the transport of user traffic.

- MR-HADDR

NEMO4G-HA supports a potential “dummy” MR-HADDR address that would be configured in every MR within the same Enterprise or across all served Enterprises (same IP address).

- Dynamic advertisement of WAN-IP Pools and learned LAN prefixes

eBGP is used to advertise the Enterprise WAN-IP Pools and the LAN prefixes learned via NEMO for the associated Enterprise.

- N-MHAE credentials

NEMO4G-HA supports local authentication for the NEMO MIPv4 RRQ based on preconfigured N-MHAE-SPI/KEY values on a per Enterprise basis (one unique set for all MRs belonging to the same Enterprise) or on a global basis (one unique set for all Enterprises).

- LAN prefixes

- NEMO4G-HA accepts a minimum of zero LAN prefixes and a maximum of eight prefixes per mobile router. Anything beyond eight prefixes shall be silently discarded.
- NEMO4G-HA supports any prefix length (including /32).
- NEMO4G-HA supports dynamic prefix updates.
  - NEMO4G-HA removes from the associated Enterprise VRF routing table any prefixes that are not included in a scheduled or ad-hoc NEMO MIPv4 re-registration request from a given MR (assuming these were present in a previous NEMO MIPv4 RRQ). E-PGW shall update the external VRF router of the removal of such prefixes on the next eBGP update.
  - NEMO4G-HA accepts and installs any new prefixes that are included in a scheduled or ad-hoc NEMO MIPv4 re-registration request to the associated Enterprise VRF routing table, as long as it doesn't exceed the maximum number of supported prefixes per MR (up to eight). E-

PGW shall update the external VRF router of the newly installed prefixes on the next eBGP update. NEMO4G-HA shall accept NEMO MIPv4 RRQs that do not include any prefixes in the first initial RRQ and it shall accept prefixes advertised in subsequent RRQs.

- In case of a prefix whose IP address or mask is changed on the MR, the MR will remove the old IP address/mask and add the new IP address/mask prefix in a scheduled or ad-hoc NEMO MIPv4 re-registration request and NEMO4G-HA shall remove the old route and add the new route corresponding to the new prefix to the Enterprise VRF routing table
- Overlapping IP addressing
  - NEMO4G-HA supports private and overlapping IP addressing across multiple Enterprises for the WAN IP pools, MR-HADDR, and LAN prefixes.

## NEMO MR Authorization

NEMO4G-HA authorizes a NEMO MIPv4 session only if a NEMO permission has been assigned to the underlying PDN connection. NEMO permission should be assigned to the underlying PDN connection via either local configuration (APN parameter) or based on a NEMO permission AVP assigned by the 3GPP AAA during the PDN authorization. For local configuration, a new APN parameter is supported to enable NEMO permission at the APN/PDN level within the P-GW service.

## MIPv4 NEMO Protocol

NEMO4G-HA processes a Mobile IPv4 NEMO Registration Request (RRQ) received from the MR NEMO client.

NEMO4G-HA processes the first of three Cisco-specific MIPv4 Extensions of type Normal Vendor/Org Specific Extension (NVSE) that are included in the MIPv4 NEMO RRQ. The three Cisco-specific NVSEs are placed after the MIPv4 “Identification” field and before the mandatory MIPv4 “Mobile-Home-Authentication-Extension.” NEMO4G-HA accepts the LAN prefixes (up to eight) encoded in the first Cisco-specific NVSE (vendor-type = 9). NEMO4G-HA is not expected to process the other two Cisco-specific NVSEs with vendor-type = 49, which carry the Internal Interface ID of the MR's Roaming Interface and the MR's Roaming Interface Bandwidth in Kbps, respectively.

Cisco-specific NVSEs follow RFC 3025 “Mobile IP Vendor/Organization Specific Extensions.”

## GRE Encapsulation

User traffic shall be encapsulated over a GRE tunnel between the MR NEMO client and NEMO4G-HA. The IP endpoints of the GRE tunnel shall be the IPv4 assigned to the MR modem during the Enterprise PDN connection setup and the IPv4 address of the NEMO4G-HA service on the E-PGW.

NEMO4G-HA shall remove the GRE encapsulation before it forwards the outbound traffic towards the Enterprise VPN via the associated SGi VLAN interface. Inbound traffic received through the same SGi VLAN interface shall be encapsulated into a GRE tunnel before it's passed to the E-PGW service for forwarding to the MR through the proper GTP/PMIP tunnel.

## Session Interactions

The following session interaction scenarios are supported between NEMO and the underlying PDN connection made over eHRPD or LTE access.

In the following circumstances, NEMO4G-HA shall withdraw the associated prefix routes from the Enterprise VRF routing table, update the eBGP neighbors and free up all internal resources allocated for the underlying PDN connection and NEMO session:

- When the eHRPD terminates the underlying PDN connection (PPP-VSNCP-Term-Req sent to MR and PMIP-BU with lifetime = 0 sent to E-PGW).
- When the MR terminates the PPP/PDN connection when accessing the network via eHRPD.
- After an eUTRAN (LTE) detach procedure initiated by the MR or MME.

NEMO4G-HA shall not be able to process any NEMO MIPv4 RRQs if there's no underlying PDN connection associated to those RRQs (PMIPv6 or GTP). In other words, NEMO MIPv4 RRQs can be accepted and processed only if an Enterprise PDN connection has been established with E-PGW by the mobile router.

NEMO4G-HA shall silently ignore NEMO MIPv4 RRQs if the underlying PDN connection associated to each of those RRQs does not have the NEMO permission indication. This applies to both eHRPD and LTE access.

NEMO4G-HA shall forward (not drop) user data using MIP or GRE tunneling (UDP/434 or IP Protocol/47, respectively) to the external enterprise VRF if such data is not destined to the NEMO4G-HA IP address. This applies to PDN connections that have or do not have the NEMO Permission indication. This shall also apply to both eHRPD and LTE access.

Any failure on either the authentication or authorize of a NEMO MIPv4 session shall not affect the underlying PDN connection established between the mobile router and the E-PGW via eHRPD or LTE. For example, if the security credentials do not match between the MR NEMO client and NEMO4G-HA, NEMO4G-HA can reject the NEMO MIPv4 RRQ, but the associated PDN connection shall not be terminated.

## NEMO Session Timers

NEMO4G-HA uses the registration lifetime value locally configured, even though MR's may use the maximum possible value (65534).

NEMO4G-HA can process ad-hoc NEMO RRQ messages.

## Enterprise-wide Route Limit Control

NEMO4G-HA supports a control mechanism to limit the maximum number of prefixes/routes that a given enterprise can register, including the pools for WAN IP assignments.

When the maximum number of routes is reached, a syslog message is generated. Once the number of routes goes under the limit, a syslog message is generated for notification.

## Forced Fragmentation

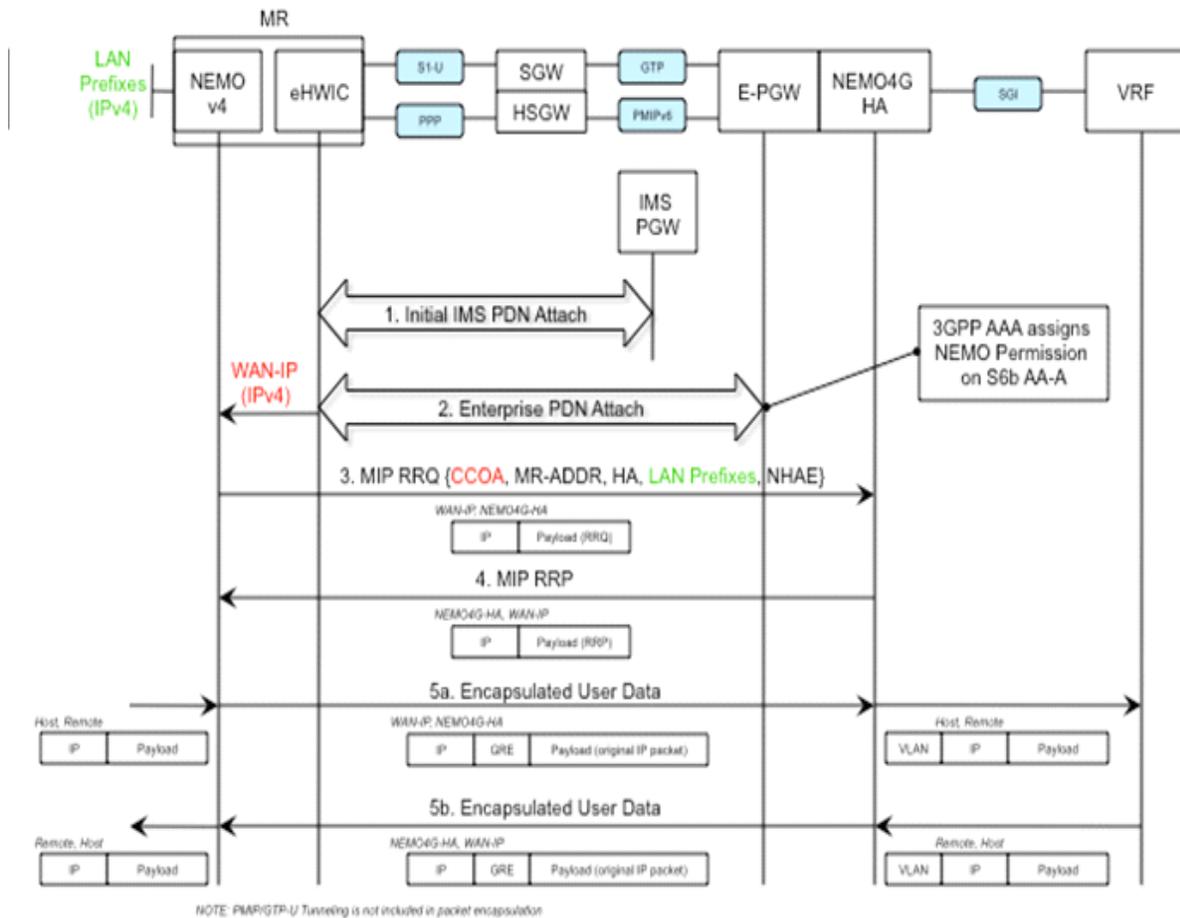
E-PGW forces IP packet fragmentation even for IP packets with the DF-bit set.

## Redundancy/Reliability

The LTE NEMO solution supports intra-chassis Session Redundancy (SR) and Inter-Chassis Session Redundancy (ICSR) functionalities.

## LTE NEMO Call Flow

The following figure describes the call flow of the NEMOv4 solution.



1. The Cisco MR eHWIC establishes first a connection to the IMS PDN to register to the LTE Network. The eHWIC's User Id must be properly provisioned on the HSS/SPR to be successfully authenticated.
2. After the Cisco MR eHWIC registers with the LTE network and establishes a connection to the IMS PDN, then it connects to the appropriate Enterprise PDN based on the locally configured Enterprise APN.
  - During the PDN authorization procedure using S6b, the 3GPP AAA assigns a NEMO permission via AVP. The AVP is also be available as an APN parameter on the E-PGW to allow NEMO service at the PDN/Enterprise level.
  - E-PGW assigns the MR eHWIC an IPv4 address from the Enterprise IPv4 pool assigned during PDN authentication.
  - E-PGW creates the proper flows internally to forward packets to the corresponding VRF external to the E-PGW platform using the IPv4 pool configuration on the egress context.
  - The MR eHWIC passed on the assigned IPv4 address to the NEMO application (also called WAN-IPv4 address).

3. The MR NEMO application initiates a Mobile IPv4 registration request (RRQ) using the following local configuration and the IPv4 address assigned to the eHWIC during the Enterprise PDN attach procedure (referred to as WAN-IP). The NEMO MIPv4 RRQ will be carried as a regular user packet over the mobility connection, either GTP in LTE and PPP/PMIPv6 in eHRPD. The NEMO MIPv4 RRQ includes the following key parameters:
  - CCOA - IPv4 address assigned to the eHWIC modem during the Enterprise PDN connection setup (WAN-IP). The MR NEMO application will use the CCOA/WAN-IP address as the source of all NEMO packets sent to NEMO4G-HA (control and tunneled user traffic).
  - MR-HADDR - Mandatory IPv4 address preconfigured in the MR NEMO application. MR-HADDR is normally used as the source of all NEMO control packets sent to the NEMO4G-HA. However, the MR NEMO application will use the CCOA as the source for all NEMO packets (control and tunneled user traffic). Therefore, NEMO4G-HA will ignore the preconfigured MR-HADDR included in the RRQ, but it will still include it in the NEMO MIPv4 RRP.
  - Home Agent Address - Preconfigured IPv4 address that the MR NEMO application uses as the destination for all NEMO control and GRE tunneled user data (NEMO4G-HA's IPv4 Address).
  - Explicit LAN Prefixes - Locally attached IPv4 networks preconfigured on the MR NEMO application. LAN prefixes will be encoded in the same Cisco NVSE extension currently used in the NEMO solution for 3G. The Cisco NVSE included in the NEMOv4 MIP RRQ is in the form of a TLV.
  - N-MHAE - Mandatory NEMO MN-HA Authentication Extension that includes the SPI and the authenticator computed using a pre-shared Key. Both SPI and Key are preconfigured in the MR NEMO application as well.
  - NEMO-Tunnel flags such as, but not limited to, "Reverse Tunnel," "Direct Termination," "Tunnel Encapsulation" = GRE.
4. NEMO4G-HA sends a MIP registration response (RRP) back to the MR after it performs the following tasks:
  - Authenticate the RRQ using the N-MHAE information included in the RRQ.
  - Authorize the NEMO service based on the NEMO permission attribute assigned to the associated Enterprise PDN connection.
  - Accept the prefixes advertised in the Cisco NVSE extension included in the NEMO MIPv4 RRQ.
    - The learned prefixes will have to adhere to the current rules of valid pool routes. The minimum valid mask length is /13 and pool routes can not include 0.0.0.0 or 255.255.255.255.
    - NEMO4G-HA will accept a minimum of 0 prefixes and a maximum of 8 prefixes. Anything beyond 8 prefixes will be silently discarded.
    - NEMO4G-HA will also check that the new resultant enterprise route count (total number of VRF routes) do not exceed the route limit potentially configured for the given enterprise. If the preconfigured route limit is exceeded, then NEMO4G-HA will reject the NEMO MIP RRQ. Otherwise, NEMO4G-HA will install the accepted prefixes in the internal VRF associated with the Enterprise PDN.
    - eBGP would then propagate the new NEMO routes to the external VRF as part of the next BGP update.

5. Upon receiving the NEMO MIP RRP, the MR will install a default route (0.0.0.0/0) in its routing table to route all traffic through the LTE connection.
  - Outbound packets are encapsulated over GRE using the CCOA/WAN-IP address as the source and the NEMO4G-HA-Service IPv4 address as the destination of the tunnel.
  - Inbound packets are encapsulated over GRE as well from the NEMO4G-HA to the MR NEMO application. The source of the GRE tunnel is the NEMO4G-HA-Service IPv4 address and the destination is the CCOA/WAN-IP address.

## Engineering Rules

- Up to 100 virtual routing tables per context. This allows up to 100 BGP-VPNs per context.
- Up to 5k host routes spread across multiple VRFs per BGP process. Limited to 6000 pool routes per chassis.
- Up to 1024 VRFs per chassis.

## Supported Standards

- IETF RFC 3025 (February 2001) “Mobile IP Vendor/Organization Specific Extensions”
- IETF RFC 1191 (November 1990) “Path MTU Discovery”

## NEMO Configuration

 **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 NEMO:

1. Create a VRF on the router and assign a VRF-ID by applying the example configuration in the *Create VRF with Route-distinguisher and Route-target* section.
2. Set the neighbors and address family to exchange routing information with a peer router by applying the example configuration in the *Set Neighbors and Address Family* section.
3. Redistribute connected routes between routing domains by applying the example configuration in the *Redistribute Connected Routes* section.
4. Allow the P-GW to use the NEMO service by applying the example in the *Configure and Enable NEMO in APN Profile* section.
5. Create a NEMO HA by applying the example in the *Create a NEMO HA* section.
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*.

## Sample Configuration

```
context egress

interface corpl-outbound

    ip address 192.168.1.1 255.255.255.0

#exit

ip vrf corpl

ip pool corpl-test 10.1.1.1 255.255.255.0 private vrf corpl

nexthop-forwarding-address 192.168.1.2 overlap vlanid 50

router bgp 100

    address-family ipv4 vrfcorpl

        neighbor 192.168.1.2 remote-as 300

        neighbor 192.168.1.2 allow-default-vrf-connection

        redistribute connected
```

```

#exit
#exit
context pgw
  apn nemo.corpl.com
  permission nemo
  ip context-name egress
  ip address pool name corpl_nemo_pool
#exit
#exit
context ingress
interface corpl-inbound
  ip address 192.168.1.1 255.255.255.0
#exit
  ha-service nemo
    mn-ha-spi spi-number 100 encrypted secret 01abd002c82b4a2c
    authentication mn-aaa noauth
    encapsulation allow keyless-gre
    bind address 38.0.0.2
  #end

```

## Create a VRF

Use this example to first create a VRF on the router and assign a VRF-ID.

```

configure
  context <context_name> -noconfirm
    ip vrf <vrf_name>
    ip pool <pool_name> <pool_address> private vrf <vrf_name>
    nexthop-forwarding-address <ip_address> overlap vlanid <vlan_id>

```

## Set Neighbors and Address Family

Use this example to set the neighbors and address family to exchange routing information with a peer router.

```
configure
  context <context_name>
    ip vrf <vrf_name>
      router bgp <as_number>
        ip vrf <vrf_name>
          neighbor <ip_address> remote-as <AS_num>
          address-family <type>
            neighbor <ip_address> activate
          end
```

## Redistribute Connected Routes

Use this example to redistribute connected routes between routing domains.

```
configure
  context <context_name>
    ip vrf <vrf_name>
      router bgp <as_number>
        ip vrf <vrf_name>
          address-family <type> vrf <vrf_name>
            redistribute connected
          exit
          redistribute connected
        end
```

## Configure and Enable NEMO in APN Profile

Use this example to configure and enable NEMO in an APN profile.

```
configure
  context <context_name>
```

```
apn <apn_name>
    permission nemo
ip context-name <name>
ip address pool name <pool_nme>
end
```

## Create a NEMO HA

Use this example to create a NEMO HA.

```
configure
context <context_name>
    ha-service <ha_service_name>
        mn-ha-spi spi-number <number> encrypted secret <enc_secret>
        authentication mn-aaa noauth
        encapsulation allow keyless-gre
        bind address <ip_address>
    end
```

# Chapter 4

## Configuring Subscriber Session Tracing

---

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 EPS 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.

This chapter discusses following topics for feature support of Subscriber Session Tracing in LTE service:

- [Introduction](#)
- [Supported Standards](#)
- [Subscriber Session Tracing 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 LTE 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 EPC network entities like MME, S-GW, P-GW support 3GPP standards based session level trace capabilities to monitor all call control events on the respective monitored interfaces including S6a, S1-MME and S11 on MME, S5, S8, S11 at S-GW and S5 and S8 on P-GW. The trace can be initiated using multiple methods:

- Management initiation via direct CLI configuration
- Management initiation at HSS with trace activation via authentication response messages over S6a 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 where the EPC 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.

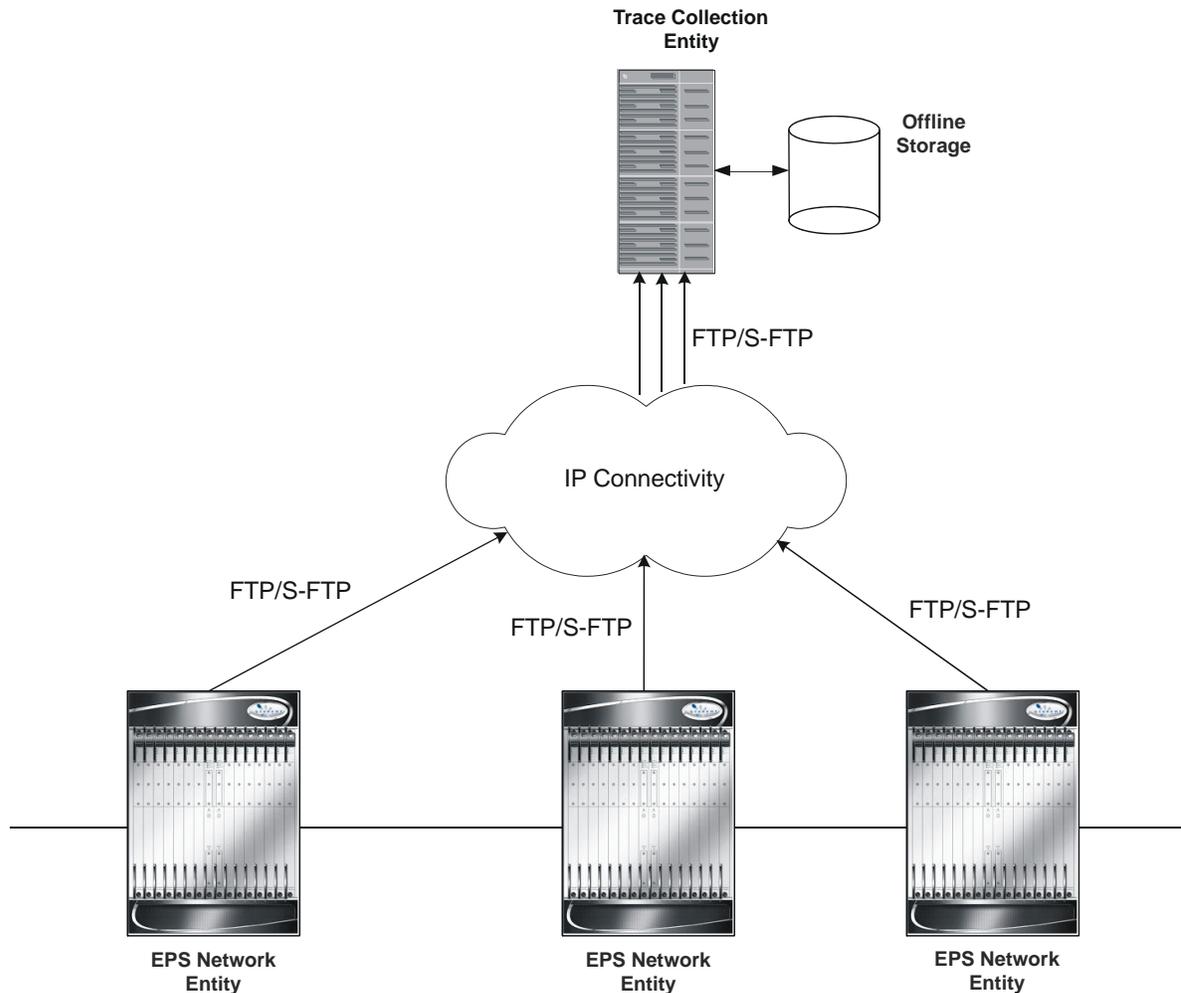


**Important:** Only Maximum Trace Depth is supported in the current release.

---

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

Figure 17. 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 network.
  - Trace of specific subscriber identified by IMSI
  - Trace of UE identified by IMEI(SV)
- 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
- Statistics and State Support
- Session Trace Details
- Management and Signaling-based activation models
- Trace Parameter Propagation
- Trace Scope (EPS Only)
  - MME: S1, S3, S6a, S10, S11
  - S-GW: S4, S5, S8, S11, Gxc
  - PDN-GW: S2a, S2b, S2c, S5, S6b, Gx, S8, SGi
- 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 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)

# Subscriber Session Trace Functional Description

This section describes the various functionality involved in tracing of subscriber session on EPC 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 AGW. Examples of NEs are the MME, S-GW, and P-GW.

Currently, subscriber session trace is not supported for co-located network elements in the EPC 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 or 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).

 **Important:** 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.

### MME

The MME support tracing of the following interfaces with the following trace capabilities:

Interface Name	Remote Device	Trace Signaling (De)Activation RX	Trace Signaling (De)Activation TX
S1a	eNodeB	N	Y
S3	SGSN	Y	Y
S6a	HSS	Y	N
S10	MME	Y	Y
S11	S-GW	N	Y

### S-GW

The S-GW support tracing of the following interfaces with the following trace capabilities:

Interface Name	Remote Device	Trace Signaling (De)Activation RX	Trace Signaling (De)Activation TX
S1-U	eNodeB	Y	N
S4	SGSN	N	N
S5	P-GW (Intra-PLMN)	Y	N
S8	P-GW (Inter-PLMN)	N	N
S11	MME	Y	N
S12	RNC	Y	N

Interface Name	Remote Device	Trace Signaling (De)Activation RX	Trace Signaling (De)Activation TX
Gxc	Policy Server	Y	N

## P-GW

The P-GW support tracing of the following interfaces with the following trace capabilities:

Interface Name	Remote Device	Trace Signaling (De)Activation RX	Trace Signaling (De)Activation TX
S2abc	Various NEs	N	N
S5	S-GW (Intra-PLMN)	Y	N
S6b	AAA Server/Proxy	Y	N
S8	S-GW (Inter-PLMN)	N	N
Gx	Policy Server	Y	N
SGi	IMS	Y	N

## 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 LTE/EPC networks.

 **Important:** This section provides the minimum instruction set to enable the Subscriber Session Trace functionality to collect session traces on network elements on EPC 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 EPC network element by applying the example configurations presented in the *Enabling Subscriber Session Trace on EPC 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** 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 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 EPC 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 | mme | pgw | sgw } { 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 to the **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 subscriber network-element { all | ggsn | mme | pgw | sgw } [
  collection-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 to the **session trace** command in the *Command Line Interface Reference*.

## 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 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 EPC 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:

```
MME
Trace Reference: 310012012345
Trace Reference: 310012012346
SGW
Trace Reference: 310012012345
Trace Reference: 310012012346
PGW
```

Trace Reference: 310012012347



# Chapter 5

## Monitoring the Service

---

This chapter provides information for monitoring service status and performance using the **show** commands found in the Command Line Interface (CLI). These commands 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 provide 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* 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 *Counters and Statistics Reference*.

Table 17. System Status and Performance Monitoring Commands

To do this:	Enter this command:
<b>View Congestion-Control Information</b>	
View Congestion-Control Statistics	<code>show congestion-control statistics {allmgr   ipsecmgr}</code>
<b>View GTP Information</b>	
View eGTP-C service statistics for a specific service	<code>show egtpc statistics egtpc-service name</code>
View GTP-U service statistics for all GTP-U data traffic on the system	<code>show gtpu statistics</code>
<b>View Infrastructure-DNS Queries</b>	
Verify Infrastructure-DNS queries to resolve P-CSCF FQDN	<code>dns-client query client-name client_name query-type AAAA query-name &lt;p-cscf.com&gt;</code>
<b>View IP Information</b>	
Display BGP Neighbors	
Verify BGP neighbors on egress P-GW context	<code>context egress_pgw_context_name show ip bgp summary</code>
Verify BGP neighbors on ingress P-GW context	<code>context ingress_pgw_context_name show ip bgp summary</code>
Display IP Connectivity State	
Verify IP connectivity to the diameter servers for various components/interfaces; all peers should be in OPEN or WAIT_DWR state	<code>show diameter peers full all  grep State</code>
Display IP Interface Status	
Verify IP interfaces are up on each context	<code>show ip interface summary show ipv6 interface summary</code>
Display IP Pool Configuration	
Verify IPv4 pools have been created and are available	<code>context egress_pgw_context_name show ip pool summary</code>
Verify IPv6 pools have been created and are available	<code>context egress_pgw_context_name show ipv6 pool summary</code>
<b>View LMA Service Information</b>	

To do this:	Enter this command:
View LMA service statistics for a specific service	<code>show lma-service statistics lma-service service_name</code>
<b>View P-GW Service Information</b>	
View P-GW service statistics	<code>show pgw-service statistics all</code>
Verify P-GW services	<code>context ingress_pgw_context_name show pgw-service all  grep Status show lma-service all  grep Status show egtp-service all  grep Status show gtpu-service all  grep State</code>
<b>View QoS/QCI Information</b>	
View QoS Class Index to QoS mapping tables	<code>show qci-qos-mapping table all</code>
<b>View RF Accounting Information</b>	
Confirm the PGW is sending Rf accounting records: <ul style="list-style-type: none"> <li>• Verify “Message sent” is non-zero</li> <li>• Verify active charging sessions are present</li> </ul>	<code>show diameter accounting servers  grep Message show active-charging sessions all  more</code>
<b>View Session Subsystem and Task Information</b>	
Display Session Subsystem and Task Statistics	
 <b>Important:</b> Refer to the <i>System Software Task and Subsystem Descriptions</i> appendix in 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 AAA Proxy statistics	<code>show session subsystem facility aaaproxy all</code>
View LMA Manager statistics	<code>show session subsystem facility hamgr all</code>
View Session Manager statistics	<code>show session subsystem facility sessmgr all</code>
<b>View Session Disconnect Reasons</b>	
View session disconnect reasons with verbose output	<code>show session disconnect-reasons</code>
<b>View Session Recovery Information</b>	
View session recovery status	<code>show session recovery status [ verbose ]</code>
<b>View Subscriber Information</b>	
Display NAT Information	
View the private IP assigned to the NAT user, along with any other public IPs assigned	<code>show subscriber full username user_name</code>
View NAT realms assigned to this user	<code>show subscriber full username user_name  grep -i nat</code>
View active charging flows for a specific NAT IP address	<code>show active-charging flows full nat required nat-ip ip_address</code>

To do this:	Enter this command:
Display Session Resource Status	
View session resource status	<code>show resources session</code>
View Statistics for Subscribers using LMA Services on the System	
View statistics for subscribers using a specific LMA service on the system	<code>show subscribers lma-service service_name</code>
View Statistics for Subscribers using P-GW Services on the System	
View statistics for subscribers using any P-GW service on the system	<code>show subscribers pgw-only full</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>
Display UE Attach Status	
<p>Confirm that a UE has attached:</p> <ul style="list-style-type: none"> <li>• Displays IMSI with one entry for each bearer per APN connection</li> <li>• Verify active charging sessions are present</li> <li>• Verify peers are active. Peers should correspond to S-GW EGTP addresses</li> <li>• Verify “Create Session Request” and “Create Session Response” categories are incrementing</li> <li>• Verify “Total Data Stats:” are incrementing</li> </ul> <p>eHRPD:</p> <ul style="list-style-type: none"> <li>• Verify lma-sessions are present</li> <li>• Verify “Binding Updates Received:” categories are incrementing</li> </ul>	<pre>show subscriber pgw-only imsi ue_imsi show active-charging sessions all  more show egtpc peers show egtpc statistics show gtpu statistics  eHRPD only show lma-service session username user_name show lma-service statistics</pre>

## 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 the *Command Line Reference* for detailed information on using this command.



# Appendix A

## Direct Tunnel

---

This chapter briefly describes the 3G/4G UMTS direct tunnel (DT) feature, indicates how it is implemented on various systems on a per call basis, and provides feature configuration procedures.

Products supporting direct tunnel include:

- 3G devices (per 3GPP TS 23.919 v8.0.0):
  - the Serving GPRS Support Node (SGSN)
  - the Gateway GPRS Support Node (GGSN)
- LTE devices (per 3GPP TS 23.401 v8.3.0):
  - Serving Gateway (S-GW)
  - PDN Gateway (P-GW)



**Important:** Direct tunnel 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 SGSN determines if setup of a direct tunnel is allowed or disallowed. Currently, the SGSN and S-GW are the only products that provide configuration commands for this feature. All other products that support direct tunnel do so by default.

This chapter provides the following information:

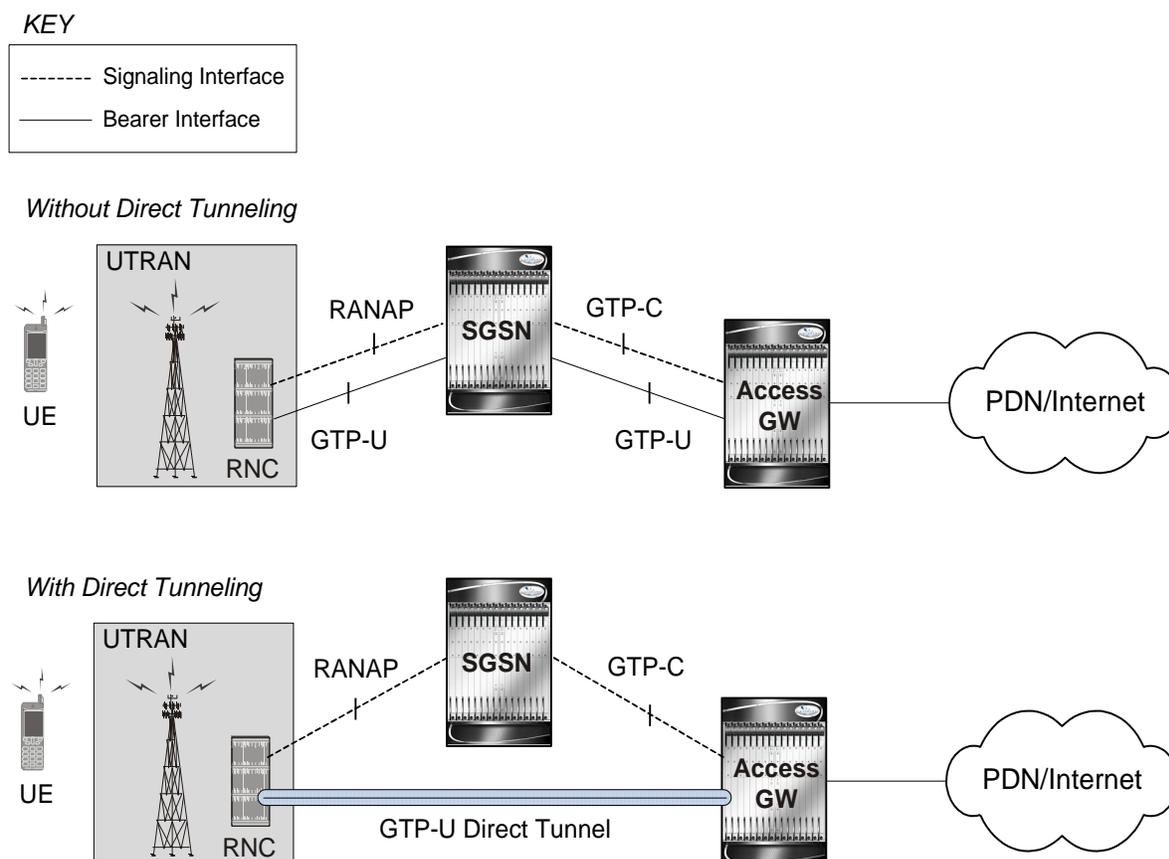
- [Direct Tunnel Feature Overview](#)
- [Direct Tunnel Configuration](#)

## Direct Tunnel Feature Overview

The direct tunnel architecture allows the establishment of a direct *user plane* (GTP-U) tunnel between the radio access network equipment (RNC) and the GGSN/P-GW.

Once a direct tunnel is established, the SGSN/S-GW continues to handle the *control plane* (RANAP/GTP-C) signaling and retains the responsibility of making the decision to establish direct tunnel at PDN context activation.

Figure 18. GTP-U Direct Tunneling



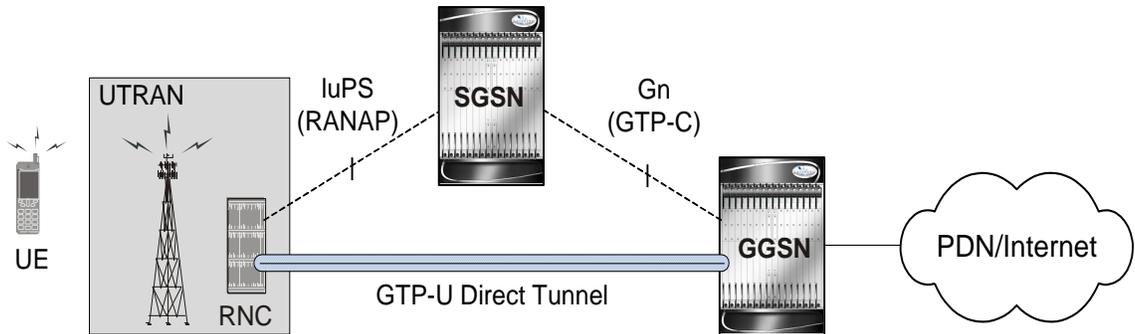
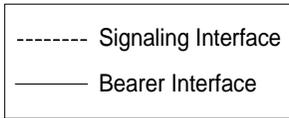
A direct tunnel improves the user experience (for example, expedites web page delivery, reduces round trip delay for conversational services) by eliminating switching latency from the user plane. An additional advantage, direct tunnel functionality implements optimization to improve the usage of user plane resources (and hardware) by removing the requirement from the SGSN/S-GW to handle the user plane processing.

A direct tunnel is achieved upon PDN context activation in the following ways:

- **3G network:** The SGSN establishes a user plane (GTP-U) tunnel directly between the RNC and the GGSN, using an Updated PDN Context Request toward the GGSN.

1..... Direct Tunneling - 3G Network

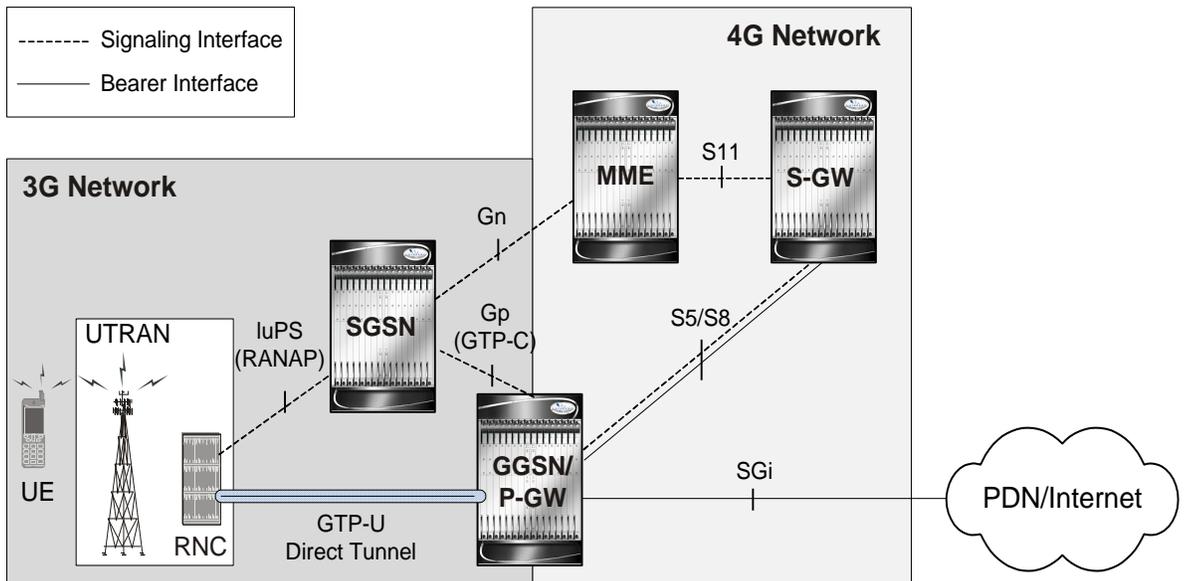
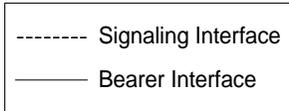
KEY



- **LTE network:** When Gn/Gp interworking with pre-release 8 (3GPP) SGSNs is enabled, the GGSN service on the P-GW supports direct tunnel functionality. The SGSN establishes a user plane (GTP-U) tunnel directly between the RNC and the GGSN/P-GW, using an Update PDN Context Request toward the GGSN/P-GW.

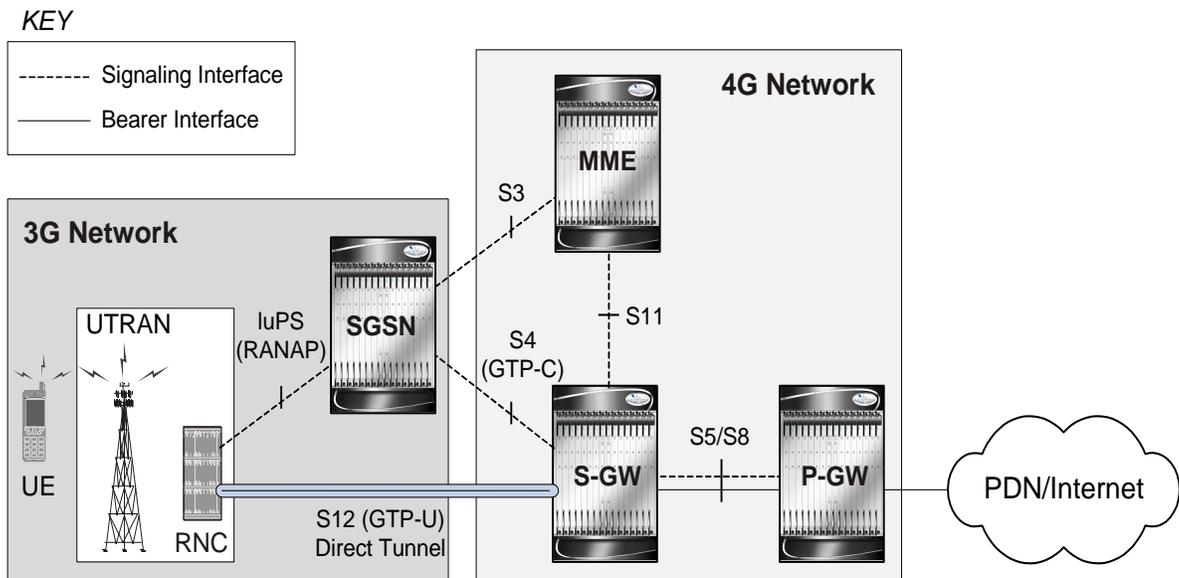
2..... Direct Tunneling - LTE Network, GTP-U Tunnel

KEY



- **LTE network:** The SGSN establishes a user plane tunnel (GTP-U tunnel over an S12 interface) directly between the RNC and the S-GW, using an Update PDN Context Request toward the S-GW.

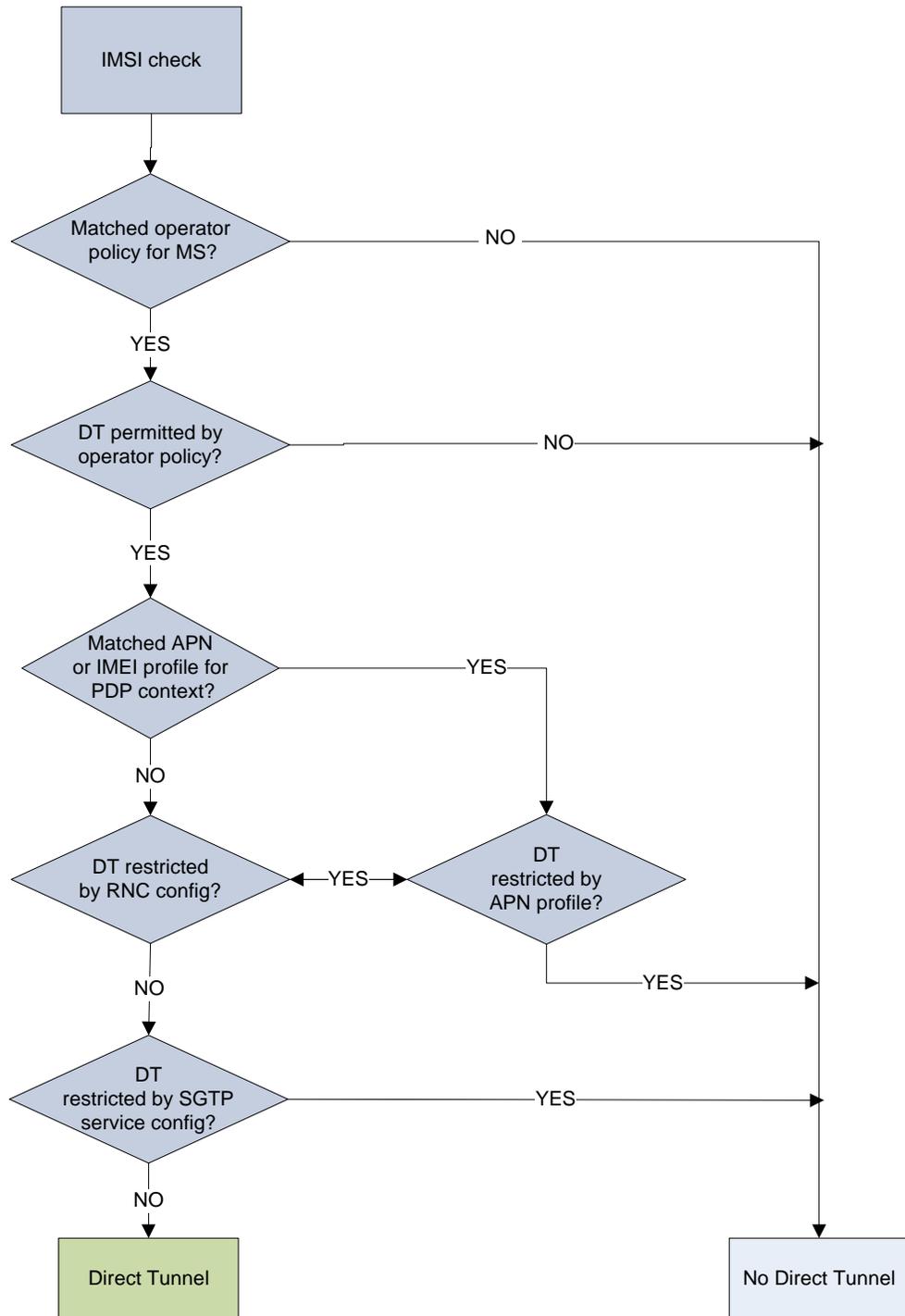
## 3.....Direct Tunneling - LTE Network, S12 Interface



A major consequence of deploying a direct tunnel is that it produces a significant increase in control plane load on both the SGSN/S-GW and GGSN/P-GW components of the packet core. Hence, deployment requires highly scalable GGSNs/P-GWs since the volume and frequency of Update PDP Context messages to the GGSN/P-GW will increase substantially. The SGSN/S-GW platform capabilities ensure control plane capacity will not be a limiting factor with direct tunnel deployment.

The following figure illustrates the logic used within the SGSN/S-GW to determine if a direct tunnel will be setup.

Figure 19. Direct Tunneling - Establishment Logic



## Direct Tunnel Configuration

The following configurations are provided in this section:

- [Configuring Direct Tunnel Support on the SGSN](#)
- [Configuring S12 Direct Tunnel Support on the S-GW](#)

### Configuring Direct Tunnel Support on the SGSN

By default, direct tunnel support is

- *disallowed* on the SGSN/S-GW
- *allowed* on the GGSN/P-GW.

The SGSN/S-GW direct tunnel functionality is enabled within an operator policy configuration. One aspect of an operator policy is to allow or disallow the setup of direct GTP-U tunnels. If no operator policies are configured, the system looks at the settings in the system operator policy named *default*.

For more information about operator policies and configuration details, refer to the *Operator Policy* chapter also in this guide.




---

**Important:** If direct tunnel is allowed in the *default* operator policy, then any incoming call that does not have an applicable operator policy configured will have direct tunnel *allowed*.

---

The following is a high-level view of the steps, and the associated configuration examples, to configure the SGSN to setup a direct tunnel.

Before beginning any of the following procedures, you must have completed (1) the basic service configuration for the SGSN, as described in the *Cisco ASR Serving GPRS Support Node Administration Guide*, and (2) the creation and configuration of a valid operator policy, as described in the *Operator Policy* chapter in this guide.

- Step 1** Configure the SGSN to setup GTP-U direct tunnel between an RNC and an access gateway by applying the example configuration presented in the *Enabling Setup of GTP-U Direct Tunnels* section below.
- Step 2** Configure the SGSN to allow GTP-U direct tunnels to an access gateway, for a call filtered on the basis of the APN, by applying the example configuration presented in the *Enabling Direct Tunnel per APN* section below.




---

**Important:** It is only necessary to complete either step 2 or step 3 as a direct tunnel can not be setup on the basis of call filtering matched with both an APN profile and an IMEI profile.

---

- Step 3** Configure the SGSN to allow GTP-U direct tunnels to a GGSN, for a call filtered on the basis of the IMEI, by applying the example configuration presented in the *Enabling Direct Tunnel per IMEI* section below.
- Step 4** Configure the SGSN to allow GTP-U direct tunnel setup from a specific RNC by applying the example configuration presented in the *Enabling Direct Tunnel to Specific RNCs* section below.
- Step 5** (*Optional*) Configure the SGSN to disallow direct tunnel setup to a single GGSN that has been configured to allow it in the APN profile. This command allows the operator to restrict use of a GGSN for any reason, such as load balancing. Refer to the `direct-tunnel-disabled-ggsn` command in the *SGTP Service Configuration Mode* chapter of the *Command Line Interface Reference*.

- 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*.
- Step 7** Check that your configuration changes have been saved by using the sample configuration found in the *Verifying the SGSN Direct Tunnel Configuration* section in this chapter.

## Enabling Setup of GTP-U Direct Tunnels

The SGSN determines whether a direct tunnel can be setup and by default the SGSN doesn't support direct tunnel.

### Example Configuration

Enabling direct tunnel setup on an SGSN is done by configuring direct tunnel support in a call-control profile.

```
config
    call-control-profile <policy_name>
        direct-tunnel attempt-when-permitted
    end
```

Notes:

- A call-control profile must have been previously created, configured, and associated with a previously created, configured, and valid operator policy. For information about operator policy creation/configuration, refer to the *Operator Policy* chapter in this guide.
- Direct tunnel is now allowed on the SGSN but will only setup if allowed on both the destination node and the RNC.

## Enabling Direct Tunnel per APN

In each operator policy, APN profiles are configured to connect to one or more GGSNs and to control the direct tunnel access to that GGSN based on call filtering by APN. Multiple APN profiles can be configured per operator policy.

By default, APN-based direct tunnel functionality is *allowed* so any existing direct tunnel configuration must be removed to return to default and to ensure that the setup has not been restricted.

### Example Configuration

The following is an example of the commands used to ensure that direct tunneling, to a GGSN(s) identified in the APN profile, is enabled:

```
config
    apn-profile <profile_name>
        remove direct tunnel
    end
```

Notes:

- An APN profile must have been previously created, configured, and associated with a previously created, configured, and valid operator policy. For information about operator policy creation/configuration, refer to the *Operator Policy* chapter in this guide.
- Direct tunnel is now allowed for the APN but will only setup if also allowed on the RNC.

## Enabling Direct Tunnel per IMEI

Some operator policy filtering of calls is done on the basis of international mobile equipment identity (IMEI) so the direct tunnel setup may rely upon the feature configuration in the IMEI profile.

The IMEI profile basis its permissions for direct tunnel on the RNC configuration associated with the IuPS service.

By default, direct tunnel functionality is *enabled* for all RNCs.

## Example Configuration

The following is an example of the commands used to enable direct tunneling in the IMEI profile:

```
config
  imei-profile <profile_name>
    direct-tunnel check-iups-service
  end
```

Notes:

- An IMEI profile must have been previously created, configured, and associated with a previously created, configured, and valid operator policy. For information about operator policy creation/configuration, refer to the *Operator Policy* chapter in this guide.
- Direct tunnel is now allowed for calls within the IMEI range associated with the IMEI profile but a direct tunnel will only setup if also allowed on the RNC.

## Enabling Direct Tunnel to Specific RNCs

SGSN access to radio access controllers (RNCs) is configured in the IuPS service.

Each IuPS service can include multiple RNC configurations that determine communications and features depending on the RNC.

By default, direct tunnel functionality is *enabled* for all RNCs.

## Example Configuration

The following is an example of the commands used to ensure that restrictive configuration is removed and direct tunnel for the RNC is enabled:

```
config
  context <ctx_name>
    iups-service <service_name>
      rnc id <rnc_id>
```

```

default direct-tunnel

end

```

Notes:

- An IuPS service must have been previously created, and configured.
- An RNC configuration must have been previously created within an IuPS service configuration.
- Command details for configuration can be found in the *Command Line Interface Reference*.

## Verifying the SGSN Direct Tunnel Configuration

Enabling the setup of a GTP-U direct tunnel on the SGSN is not a straight forward task. It is controlled by an operator policy with related configuration in multiple components. Each of these component configurations must be checked to ensure that the direct tunnel configuration has been completed. You need to begin with the operator policy itself.

## Verifying the Operator Policy Configuration

For the feature to be enabled, it must be allowed in the call-control profile and the call-control profile must be associated with an operator policy. As well, either an APN profile or an IMEI profile must have been created/configured and associated with the same operator policy. Use the following command to display and verify the operator policy and the association of the required profiles:

```
show operator-policy full name <policy_name>
```

The output of this command displays profiles associated with the operator policy.

```
[local]asr5x00# show operator-policy full name oppolicy1

Operator Policy Name = oppolicy1

Call Control Profile Name                : ccprofile1

Validity                                 : Valid

IMEI Range 99999999999990 to 99999999999995

IMEI Profile Name                        : imeiprofile1

Validity                                 : Invalid

APN NI homers1

APN Profile Name                         : apnprofile1

Validity                                 : Valid

APN NI visitors2

APN Profile Name                         : apnprofile2

Validity                                 : Invalid

```

Notes:

- Validity refers to the status of the profile. Valid indicates that profile has been created and associated with the policy. Invalid means only the name of the profile has been associated with the policy.
- The operator policy itself will only be valid if one or more IMSI ranges have been associated with it - refer to the *Operator Policy* chapter, in this guide, for details.

## Verifying the Call-Control Profile Configuration

Use the following command to display and verify the direct tunnel configuration for the call-control profiles:

```
show call-control-profile full name <profile_name>
```

The output of this command displays all of the configuration, including direct tunnel for the specified call-control profile.

```
Call Control Profile Name = ccprofile1
```

```
...
```

```
Re-Authentication : Disabled
```

```
Direct Tunnel : Not Restricted
```

```
GTPU Fast Path : Disabled
```

```
..
```

## Verifying the APN Profile Configuration

Use the following command to display and verify the direct tunnel configuration in the APN profile:

```
show apn-profile full name <profile_name>
```

The output of this command displays all of the configuration, including direct tunnel for the specified APN profile.

```
Call Control Profile Name = apnprofile1
```

```
...
```

```
IP Source Validation : Disabled
```

```
Direct Tunnel : Not Restricted
```

```
Service Restriction for Access Type > UMTS : Disabled
```

```
..
```

## Verifying the IMEI Profile Configuration

Use the following command to display and verify the direct tunnel configuration in the IMEI profile:

```
show imei-profile full name <profile_name>
```

The output of this command displays all of the configuration, including direct tunnel for the specified IMEI profile.

```
IMEI Profile Name = imeiprofile1
```

```

Black List                : Disabled
GGSN Selection            : Disabled
Direct Tunnel              : Enabled

```

## Verifying the RNC Configuration

Use the following command to display and verify the direct tunnel configuration in the RNC configuration:

```
show iups-service name <service_name>
```

The output of this command displays all of the configuration, including direct tunnel for the specified IuPS service.

```

IService name              : iups1
...
Available RNC:
  Rnc-Id                   : 1
  Direct Tunnel            : Not Restricted

```

## Configuring S12 Direct Tunnel Support on the S-GW

The example in this section configures an S12 interface supporting direct tunnel bypass of the S4 SGSN for inter-RAT handovers.

The direct tunnel capability on the S-GW is enabled by configuring an S12 interface. The S4 SGSN is then responsible for creating the direct tunnel by sending an FTEID in a control message to the MME over the S3 interface. The MME forwards the FTEID to the S-GW over the S11 interfaces. The S-GW responds with its own U-FTEID providing the SGSN with the identification information required to set up the direct tunnel over the S12 interface.

Use the following example to configure this feature:

```

configure

context <egress_context_name> -noconfirm

  interface <s12_interface_name>

    ip address <s12_ipv4_address_primary>

    ip address <s12_ipv4_address_secondary>

    exit

  exit

port ethernet <slot_number/port_number>

  no shutdown

  bind interface <s12_interface_name> <egress_context_name>

```

```
exit
context <egress_context_name> -noconfirm
    gtpu-service <s12_gtpu_egress_service_name>
        bind ipv4-address <s12_interface_ip_address>
    exit
    egtp-service <s12_egtp_egress_service_name>
        interface-type interface-sgw-egress
        validation-mode default
        associate gtpu-service <s12_gtpu_egress_service_name>
        gtpc bind address <s12_interface_ip_address>
    exit
    sgw-service <sgw_service_name> -noconfirm
        associate egress-proto gtp egress-context <egress_context_name> egtp-service
        <s12_egtp_egress_service_name>
    end
```

**Notes:**

- The S12 interface IP address(es) can also be specified as IPv6 addresses using the **ipv6 address** command.

# 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.

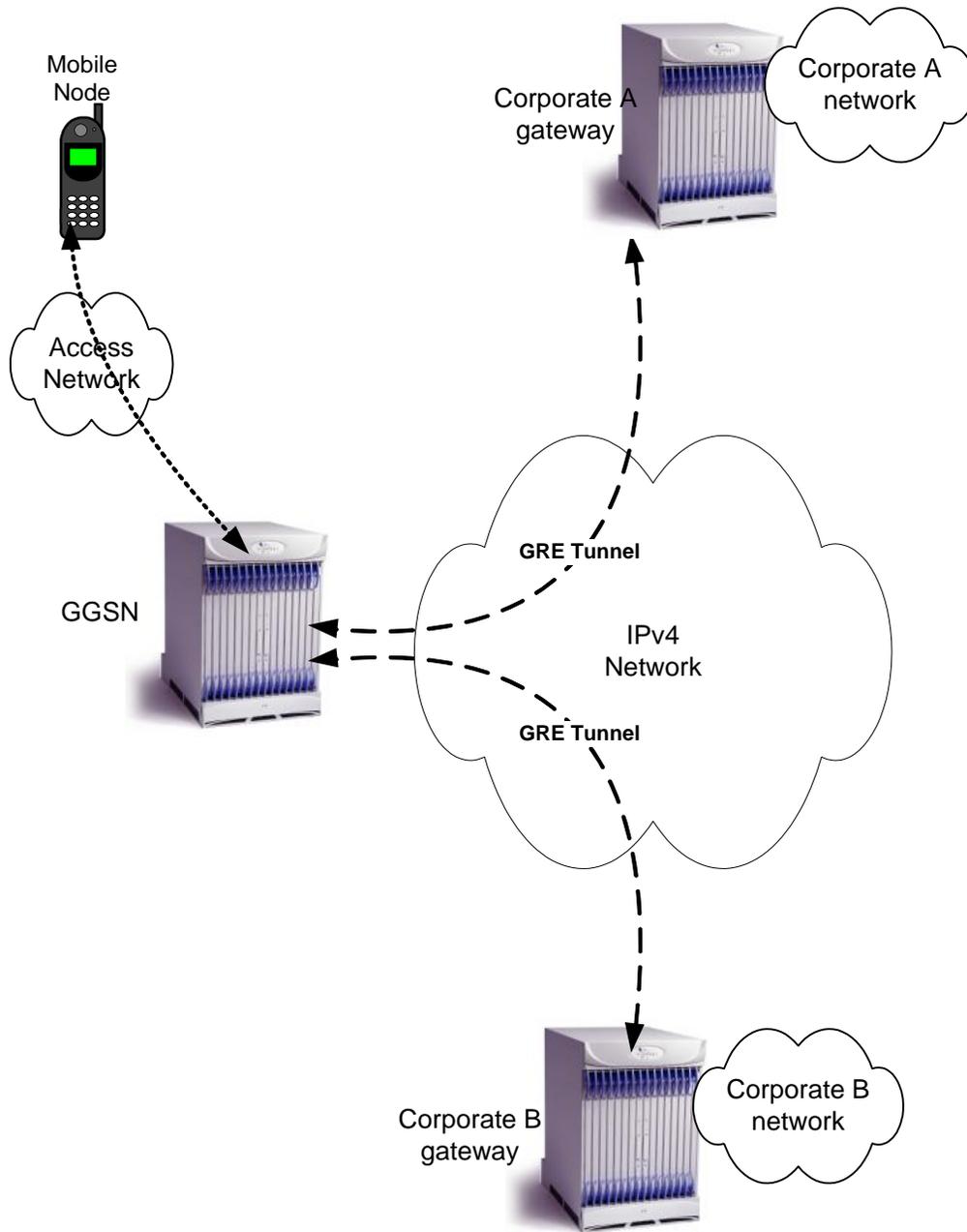
It is a common technique to enable multi-protocol local networks over a single-protocol backbone, to connect non-contiguous networks and allow virtual private networks across WANs. This mechanism encapsulates data packets from one protocol inside a different protocol and transports the data packets unchanged 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 20. 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

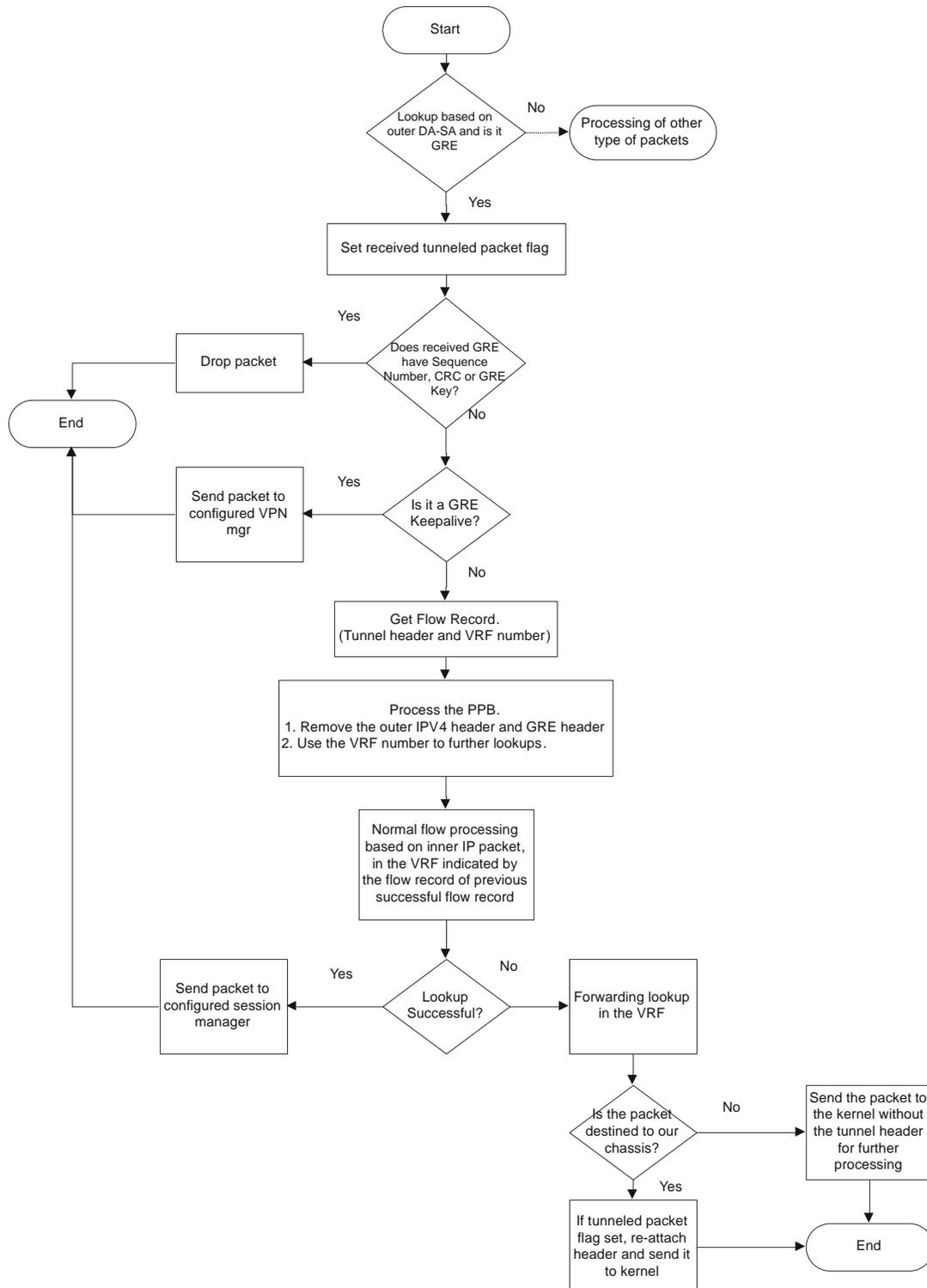
The GRE interface provides two types of data processing; one for ingress packets and another for egress packets.

### 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.

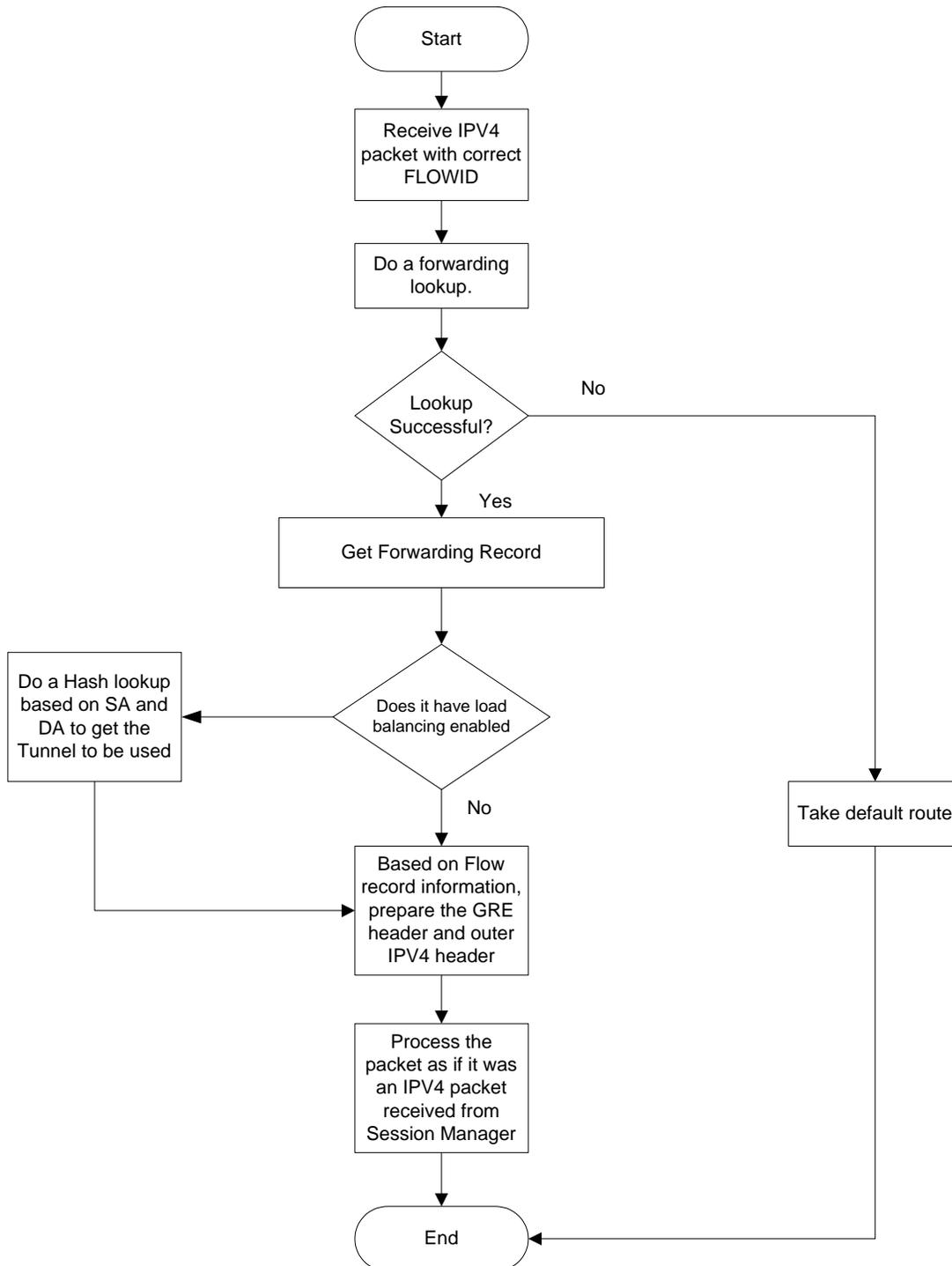
Figure 21. Ingress Packet Processing on GRE Interface



## Egress Packet Processing on GRE Interface

Figure given below provides a flow of process for outgoing packets on GRE interface:

Figure 22. 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 (foo1), 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 23. Rel. 6 Gx IMS Authorization Call Flow

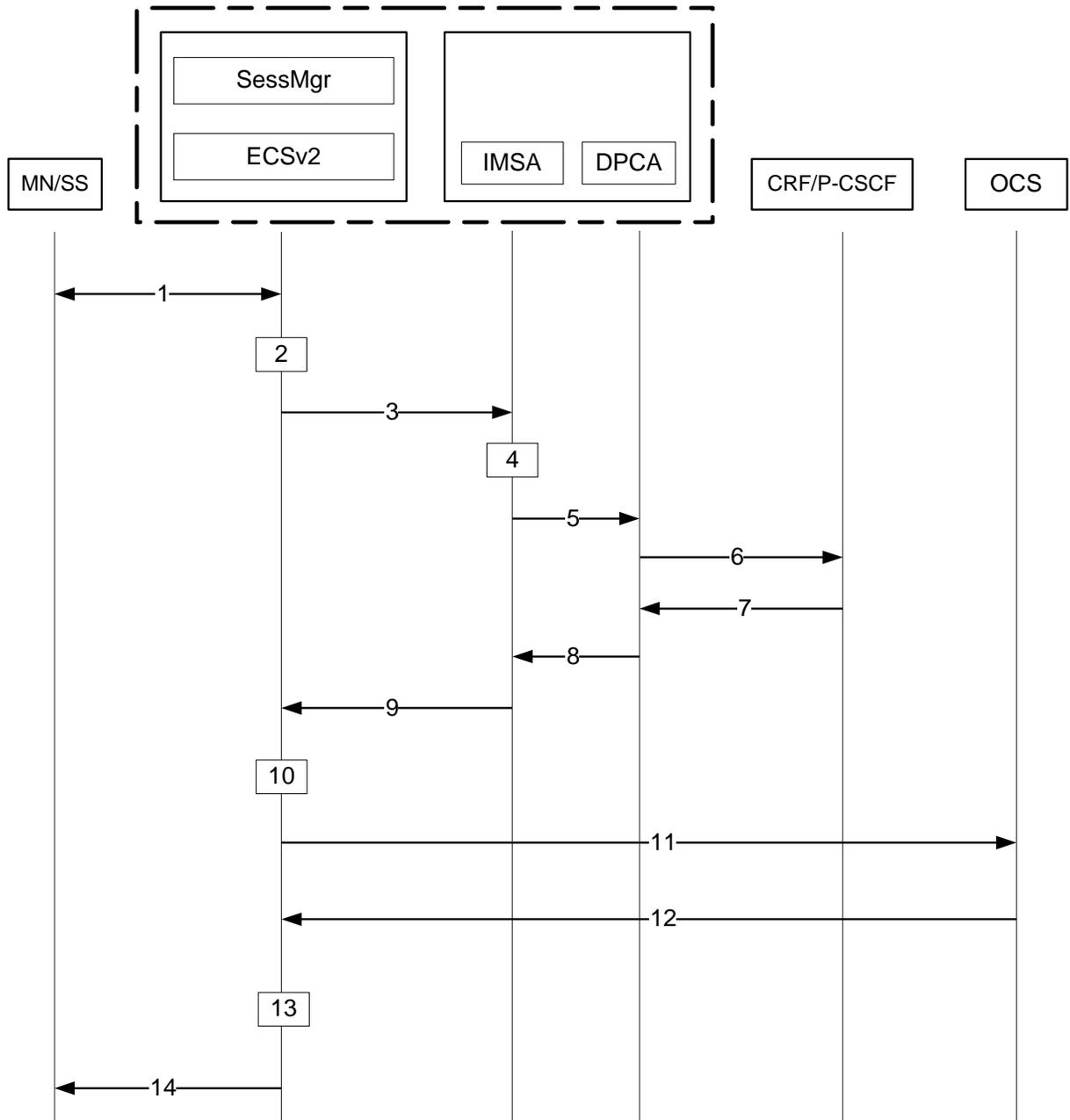


Table 18. Rel. 6 Gx IMS Authorization Call flow Description

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
- IPSP

This section describes the following topics:

- [Introduction](#)
- [Terminology and Definitions](#)
- [How it Works](#)
- [Configuring Rel. 7 Gx Interface](#)
- [Gathering Statistics](#)

### Introduction

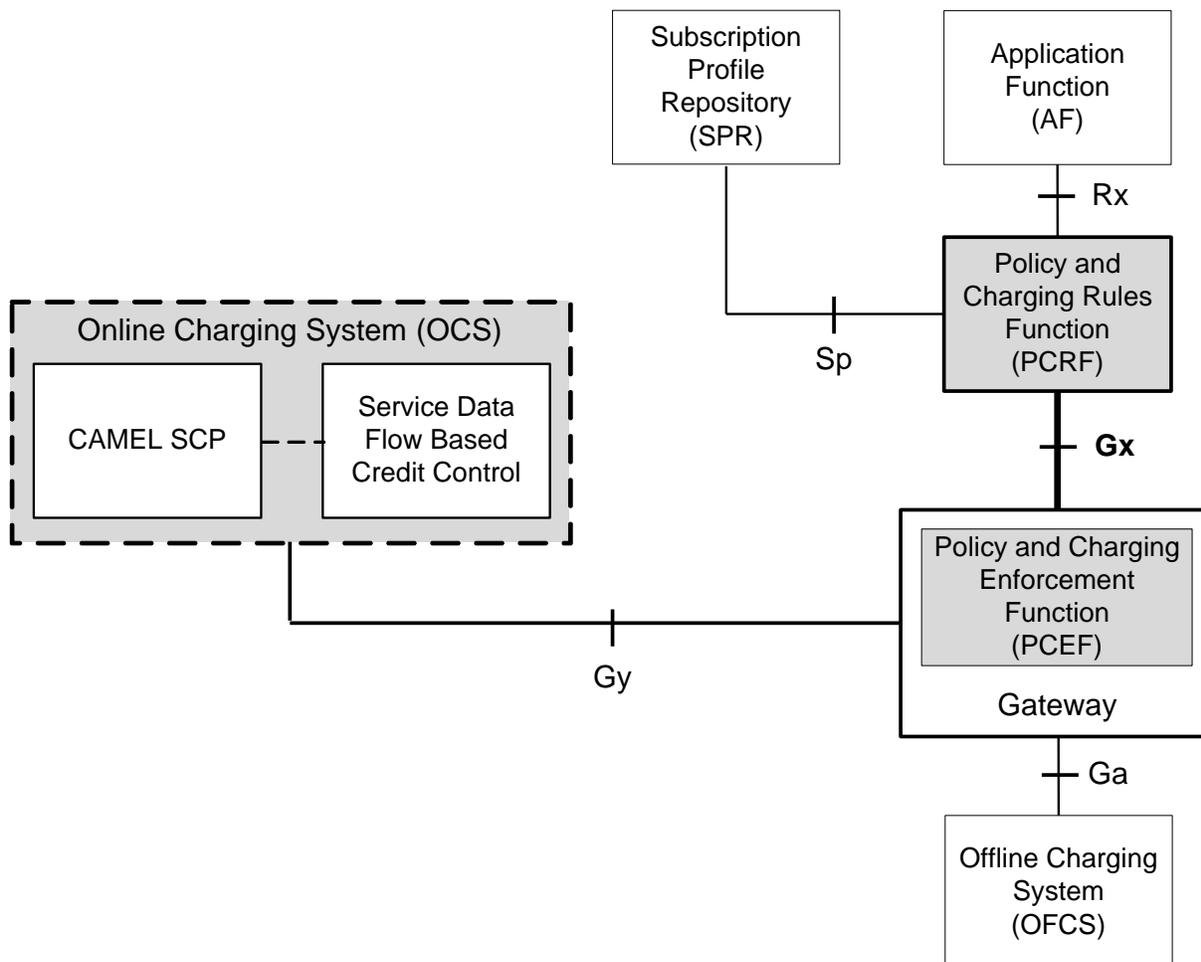
For IMS deployment in GPRS/UMTS networks the system uses Rel. 7 Gx interface for policy-based admission control support and flow-based charging. The Rel. 7 Gx interface supports enforcing policy control features like gating, bandwidth limiting, and so on, and also supports flow-based charging. This is 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.

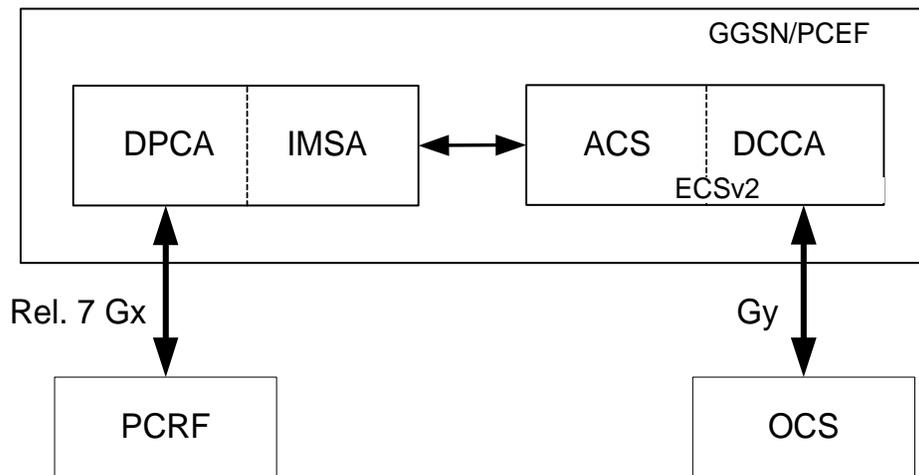
The Rel. 7 Gx reference point is located between the Gateway and the PCRF. This reference point is used for provisioning and removal of PCC rules from the PCRF to the Gateway, and the transmission of traffic plane events from the Gateway to the PCRF. The Gx reference point can be used for charging control, 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 24. 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 25. 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 IPSPG 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 IPSPG 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 a 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 26. Rel. 7 Gx IMS Authorization Call Flow

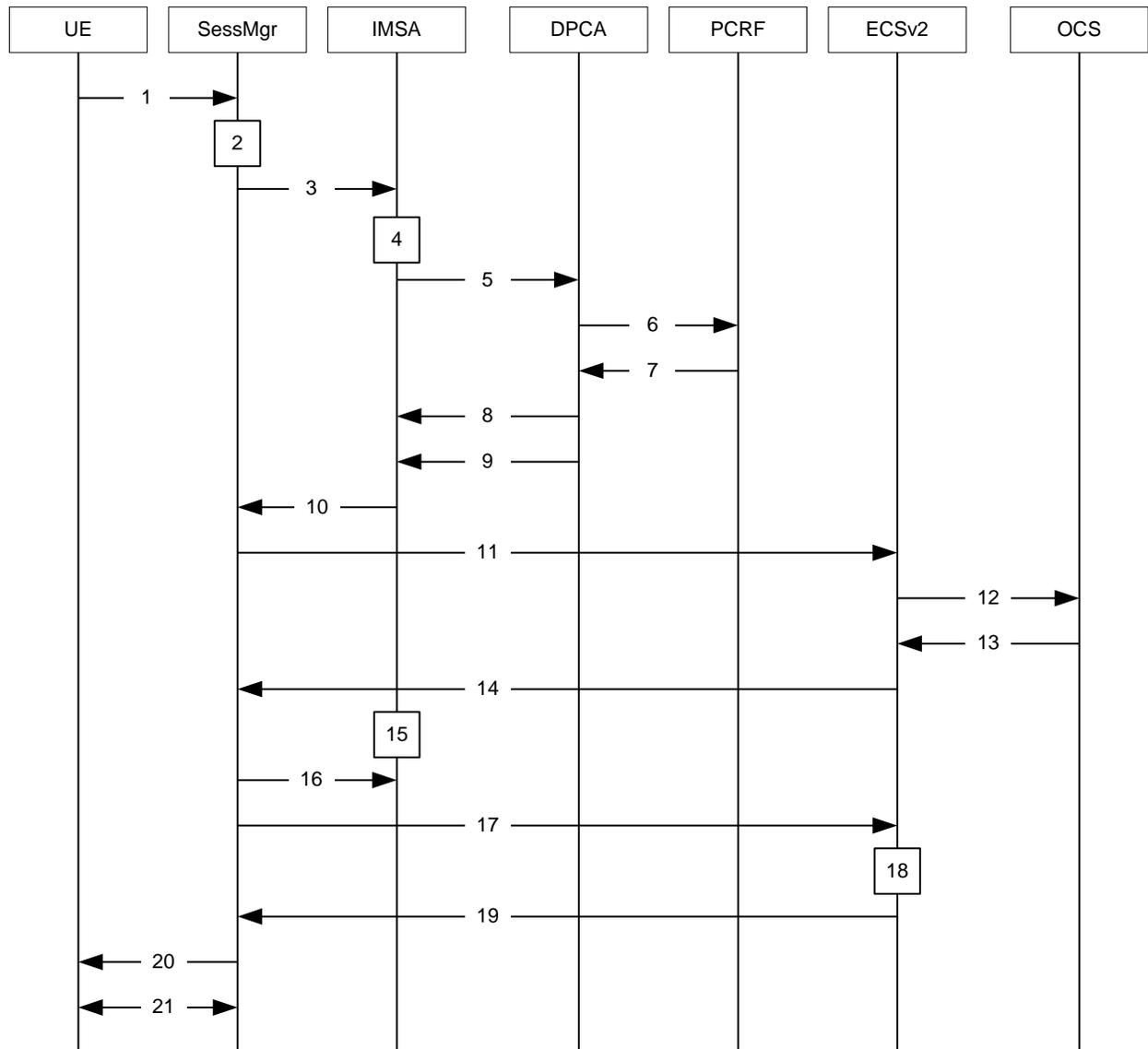


Table 19. Rel. 7 Gx IMS Authorization Call flow Description

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 20. 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/PSDSN 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

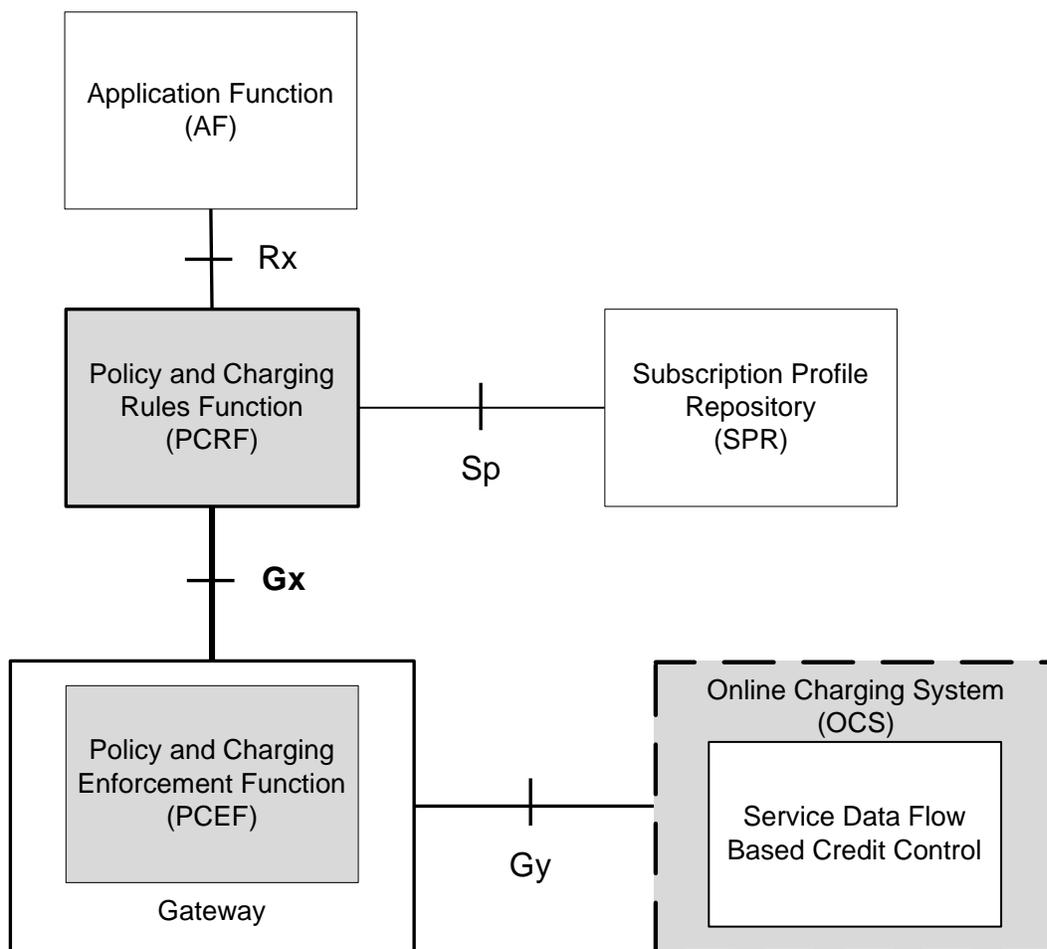
For IMS deployment in CDMA networks the system uses Rel. 8 Gx interface for policy-based admission control support and flow-based charging (FBC). The Rel. 8 Gx interface supports enforcing policy control features like gating, bandwidth limiting, and so on, and also supports FBC. This is accomplished 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.

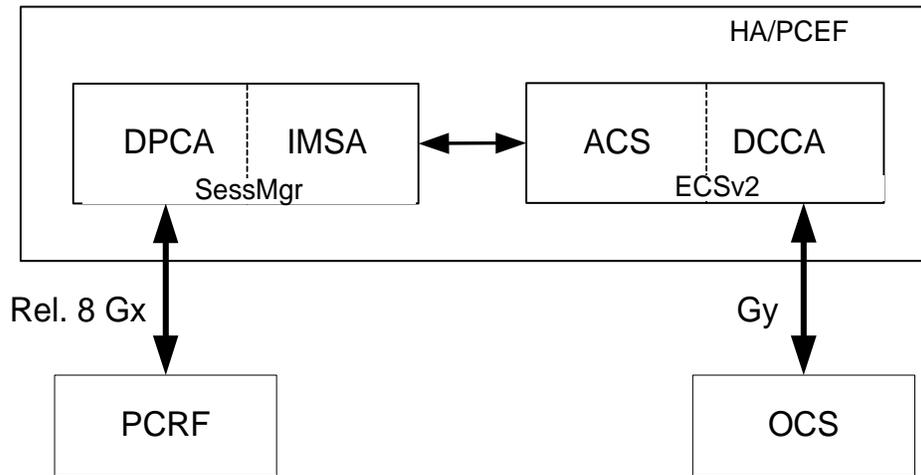
Figure 27. HA/PDSN Rel. 8 Gx PCC Logical Architecture



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 28. 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 29. HA/PDSN Rel. 8 Gx IMS Authorization Call Flow

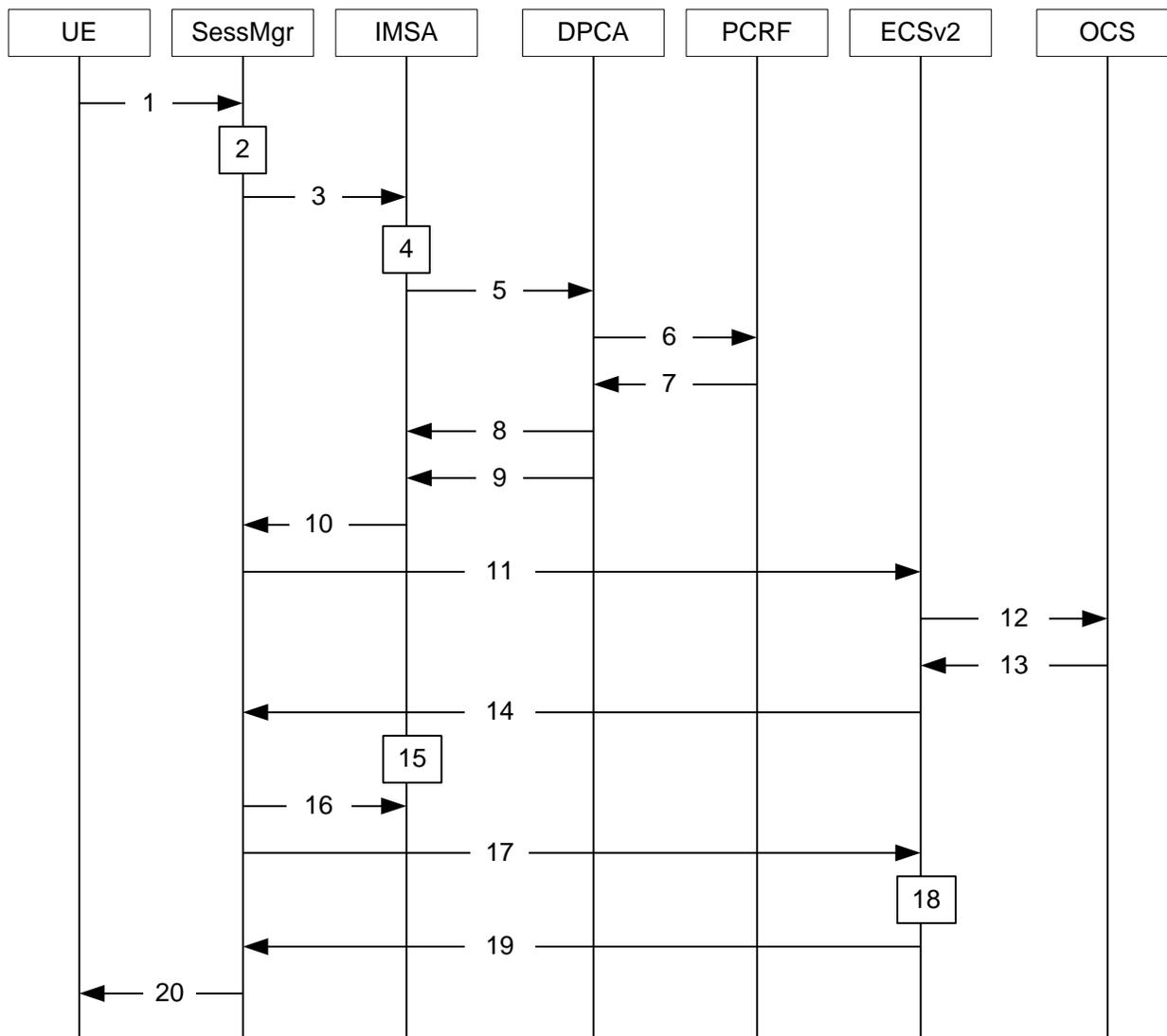


Table 21. HA/PDSN Rel. 8 Gx IMS Authorization Call flow Description

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 22. 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.	<code>show ims-authorization policy-control statistics</code>
Information and statistics specific to the authorization servers used for IMS Authorization service.	<code>show ims-authorization servers ims-auth-service</code>
Information of all IMS Authorization service.	<code>show ims-authorization service all</code>
Statistics of IMS Authorization service.	<code>show ims-authorization service statistics</code>
Information, configuration, and statistics of sessions active in IMS Authorization service.	<code>show ims-authorization sessions all</code>

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

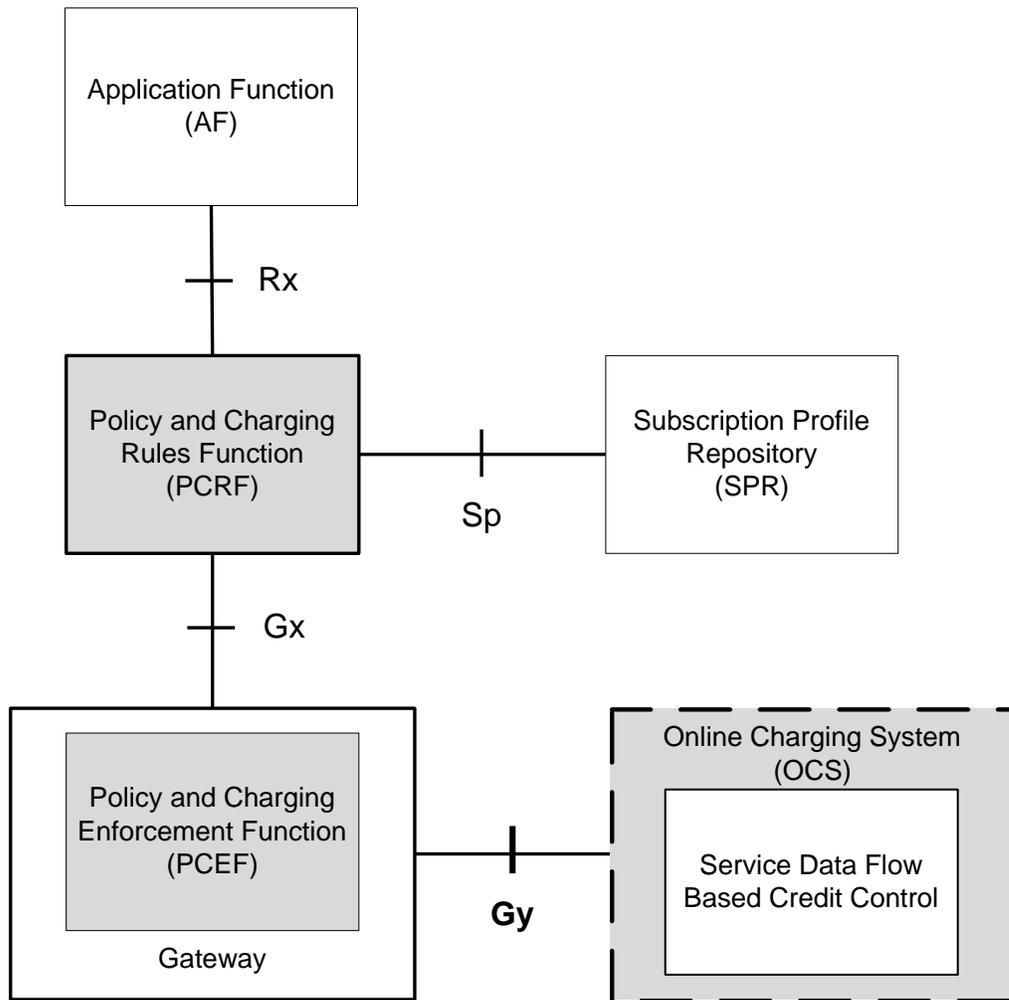
The Gy interface is the online charging interface between the PCEF/GW (Charging Trigger Function (CTF)) and the Online Charging System (Charging-Data-Function (CDF)).

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 prepaid 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.

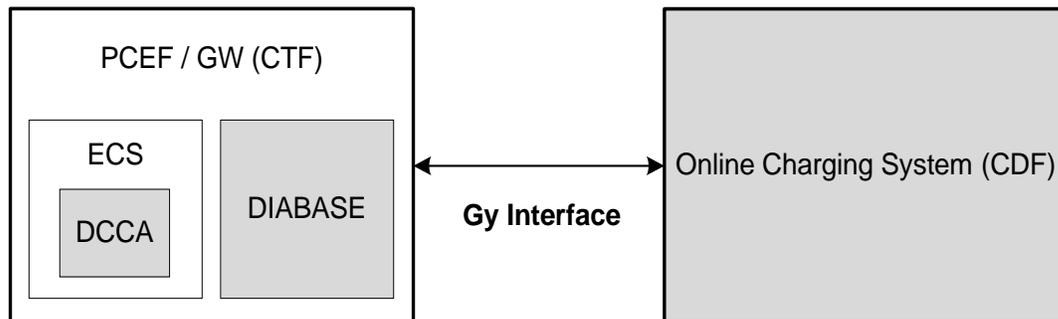
The following figure shows the Gy reference point in the policy and charging architecture.

Figure 30. 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 31. 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.

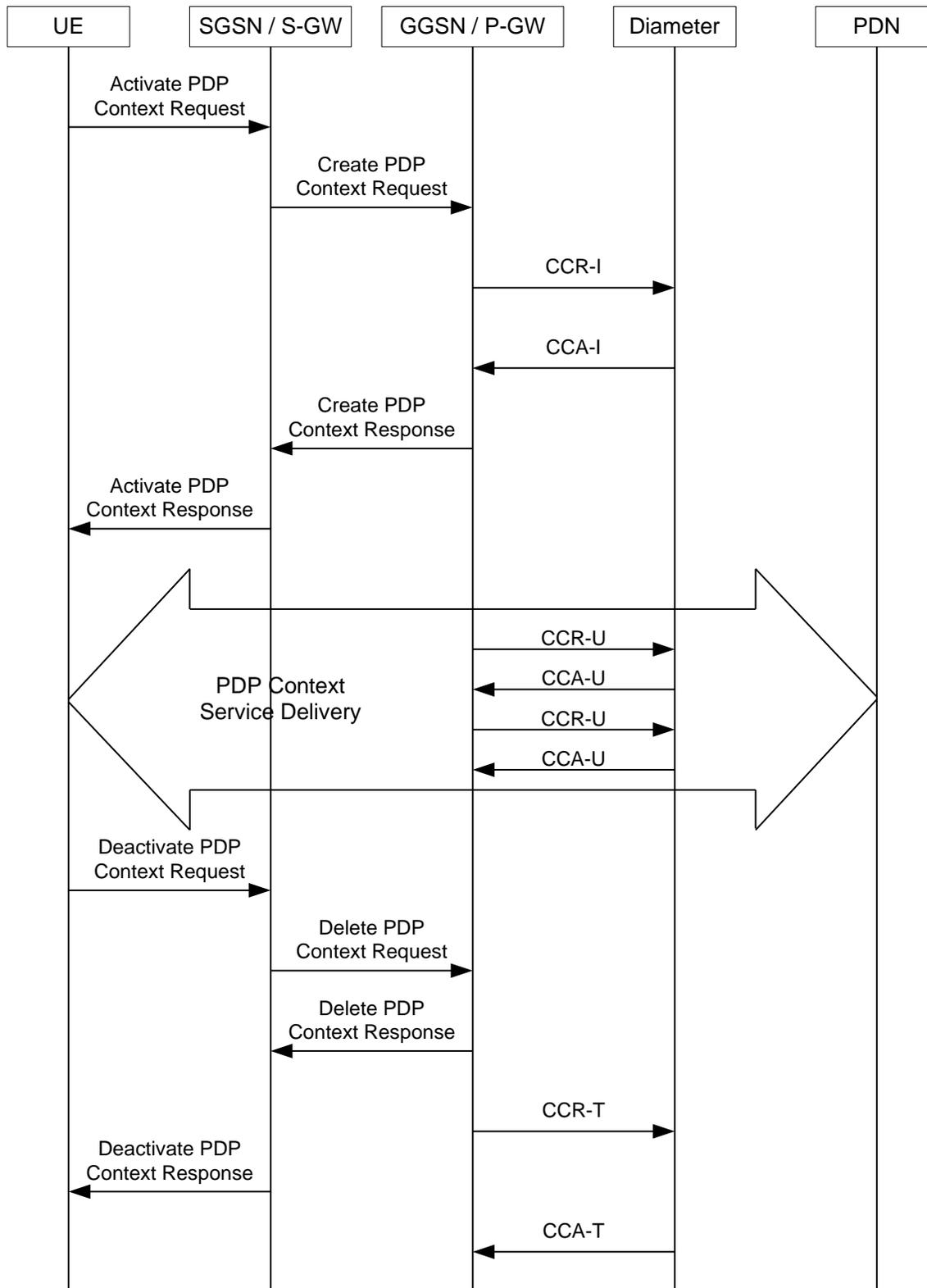
- Credit Control Request - Initial (CCR-I)
- Credit Control Request - Update (CCR-U)
- Credit Control Request - Terminate (CCR-T)
- Credit Control Answer (CCA)
- Credit Control Answer - Initial (CCA-I)
- Credit Control Answer - Update (CCA-U)

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)

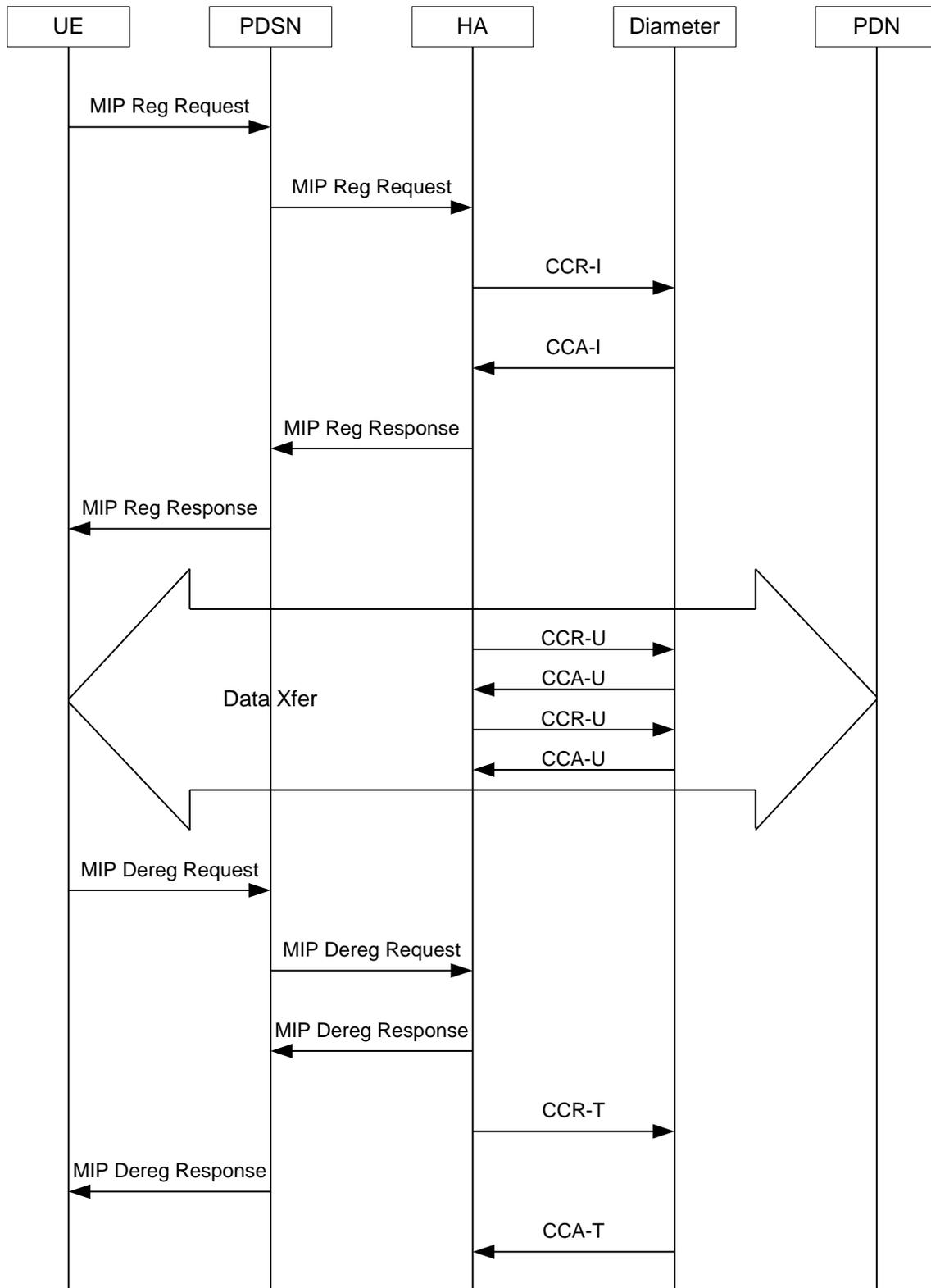
The following figure depicts the call flow for a simple call request in the GGSN / P-GW /IPSG Gy implementation.

Figure 32. 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 33. 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-Initialtion-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.	<code>show active-charging sessions full</code>
Information on all rule definitions configured in the service.	<code>show active-charging ruledef all</code>
Information on all charging actions configured in the service.	<code>show active-charging charging-action all</code>
Information on all rulebases configured in the service.	<code>show active-charging rulebase all</code>
Statistics of the Credit Control application, DCCA.	<code>show active-charging credit-control statistics</code>
States of the Credit Control application's sessions, DCCA.	<code>show active-charging credit-control session-states [ rulebase &lt;rulebase_name&gt; ] [ content-id &lt;content_id&gt; ]</code>



# 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:

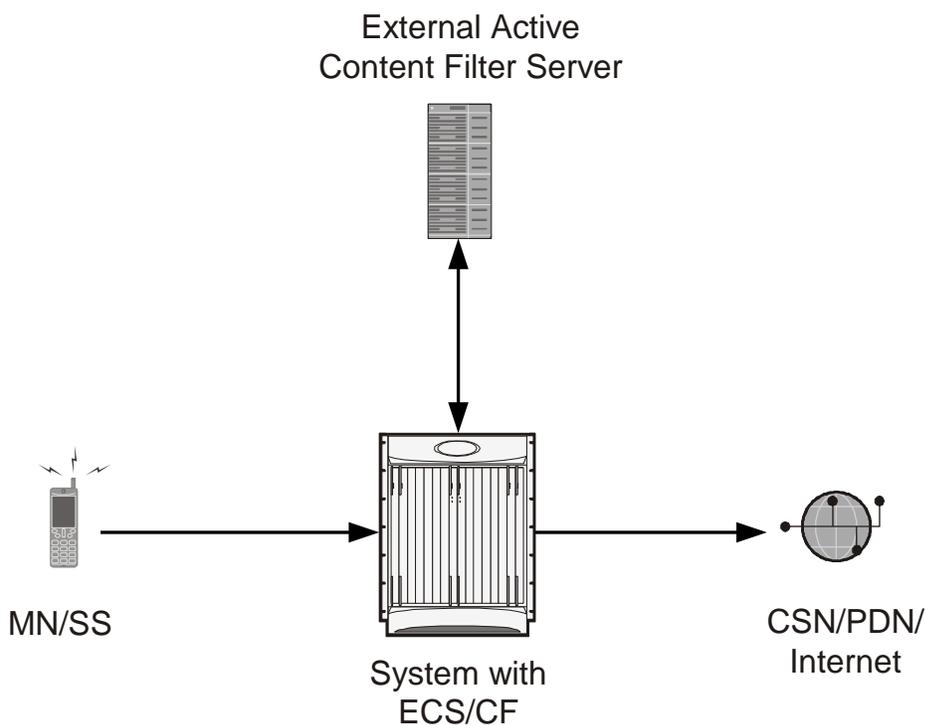
- GGSN
- P-GW

## 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 34. 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 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](#)

---

**■ Configuring ICAP Interface Support**

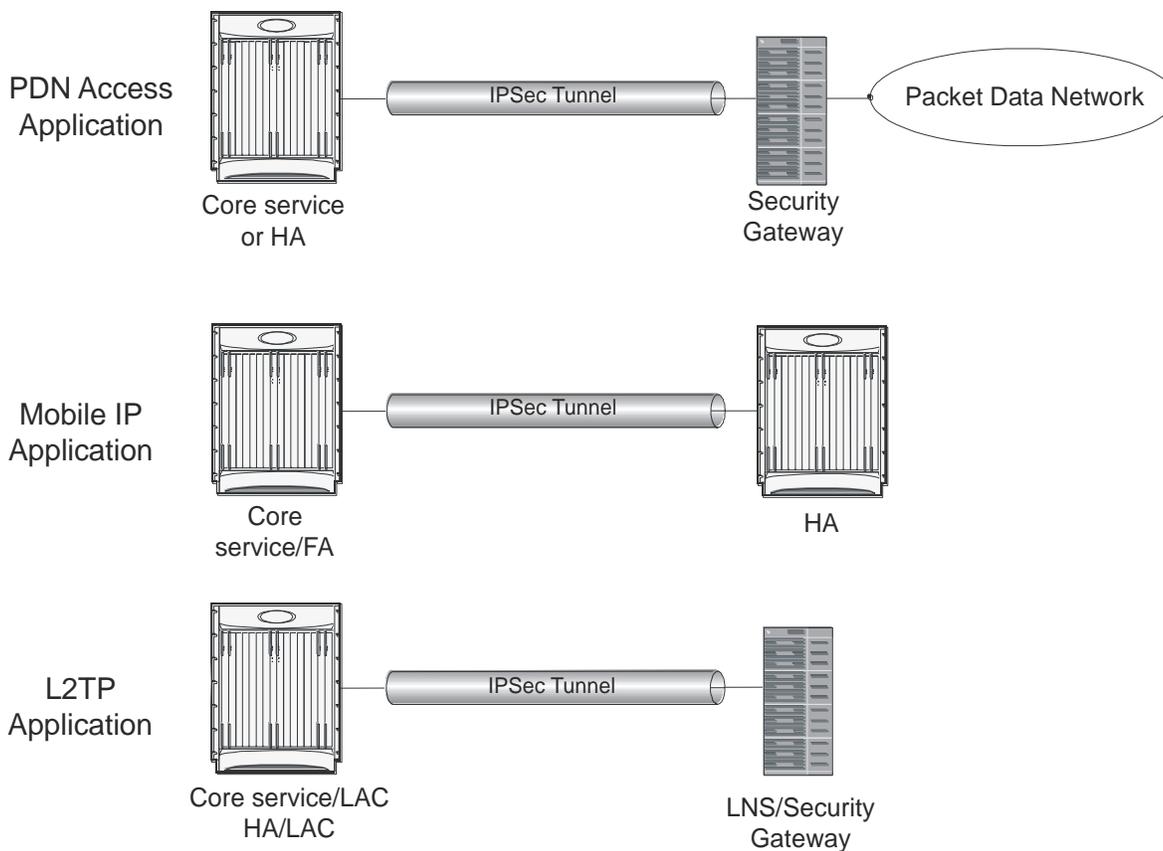
- [APN Template Configuration to Support L2TP](#)
- [IPSec for LTE/SAE Networks](#)

## 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 35. 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 36. IPSec PDN Access Processing

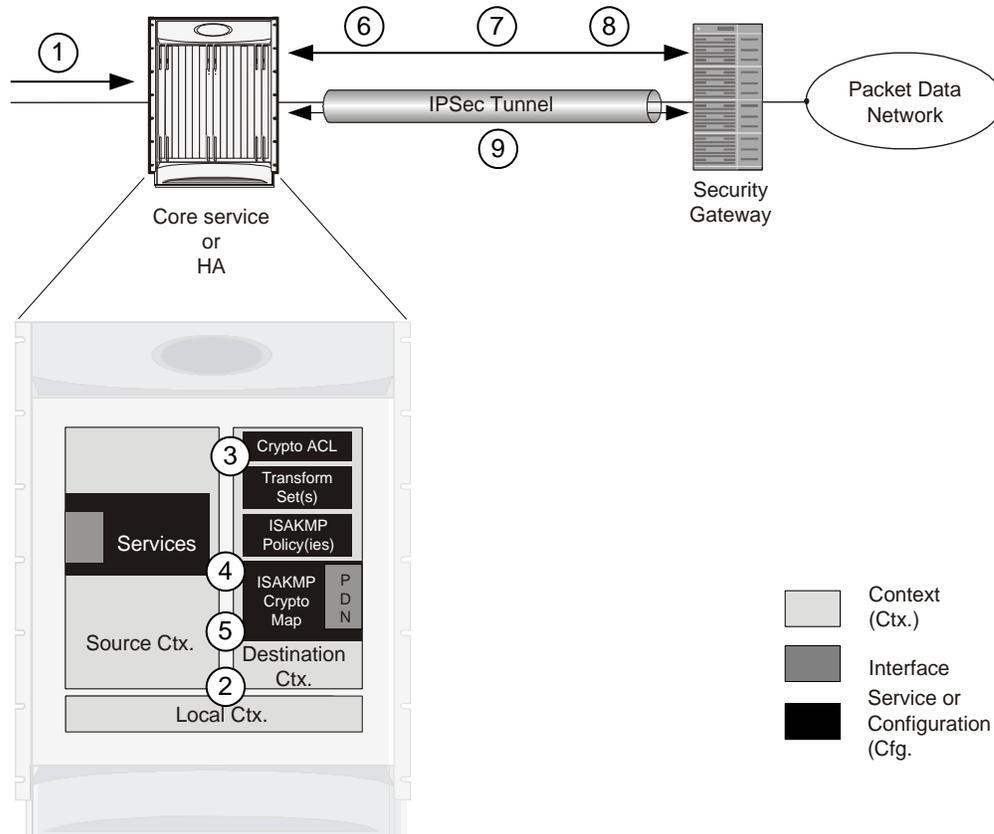


Table 23. IPSec PDN Access Processing

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 37. IPsec-based Mobile IP Session Processing

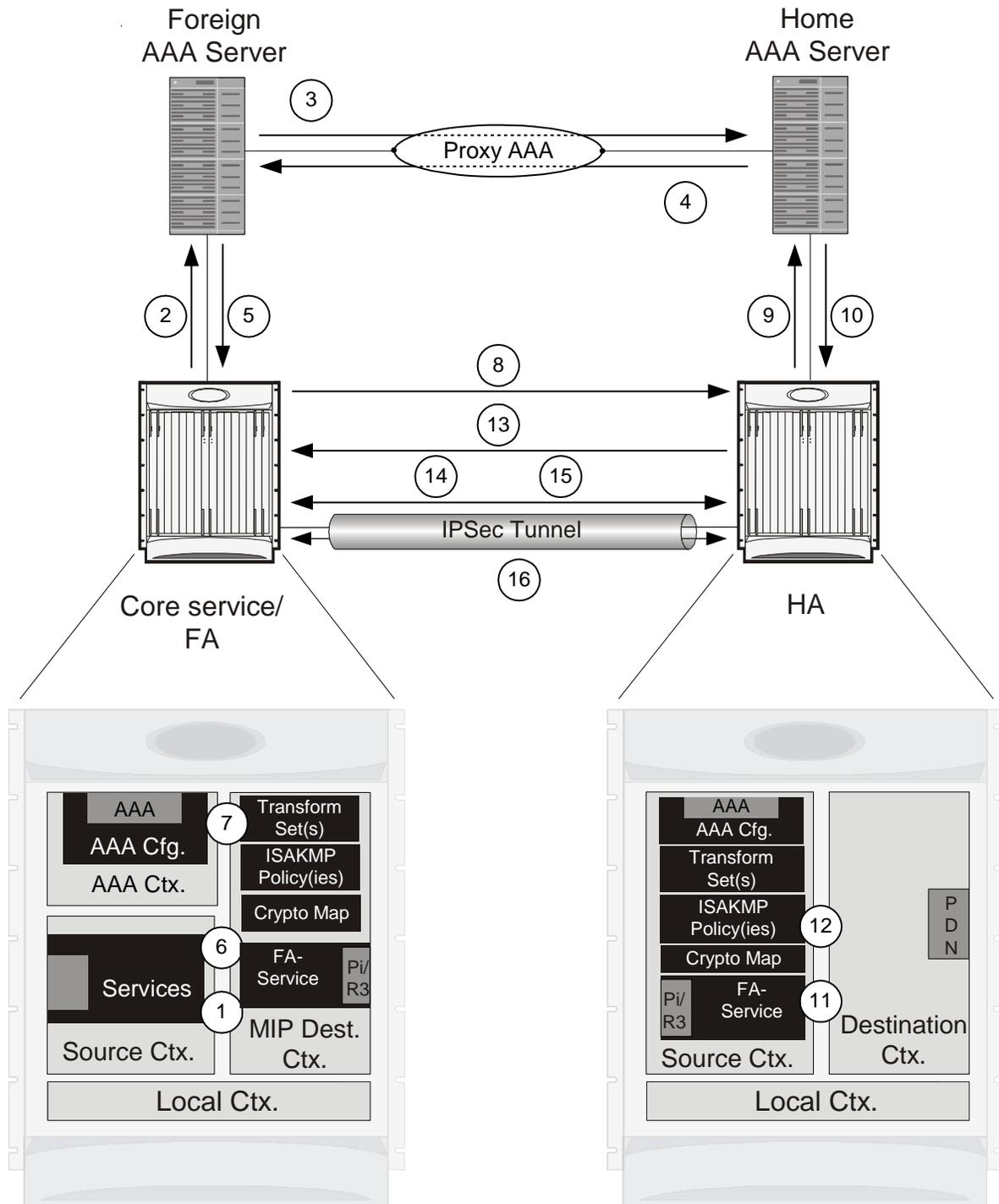


Table 24. IPsec-based Mobile IP Session Processing

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 <code>isakmp peer-ha</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>
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> <p>The password used in the access request is the RADIUS shared secret.</p>
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 on 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 on 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 38. Attribute-based L2TP, IPsec-Encrypted Session Processing

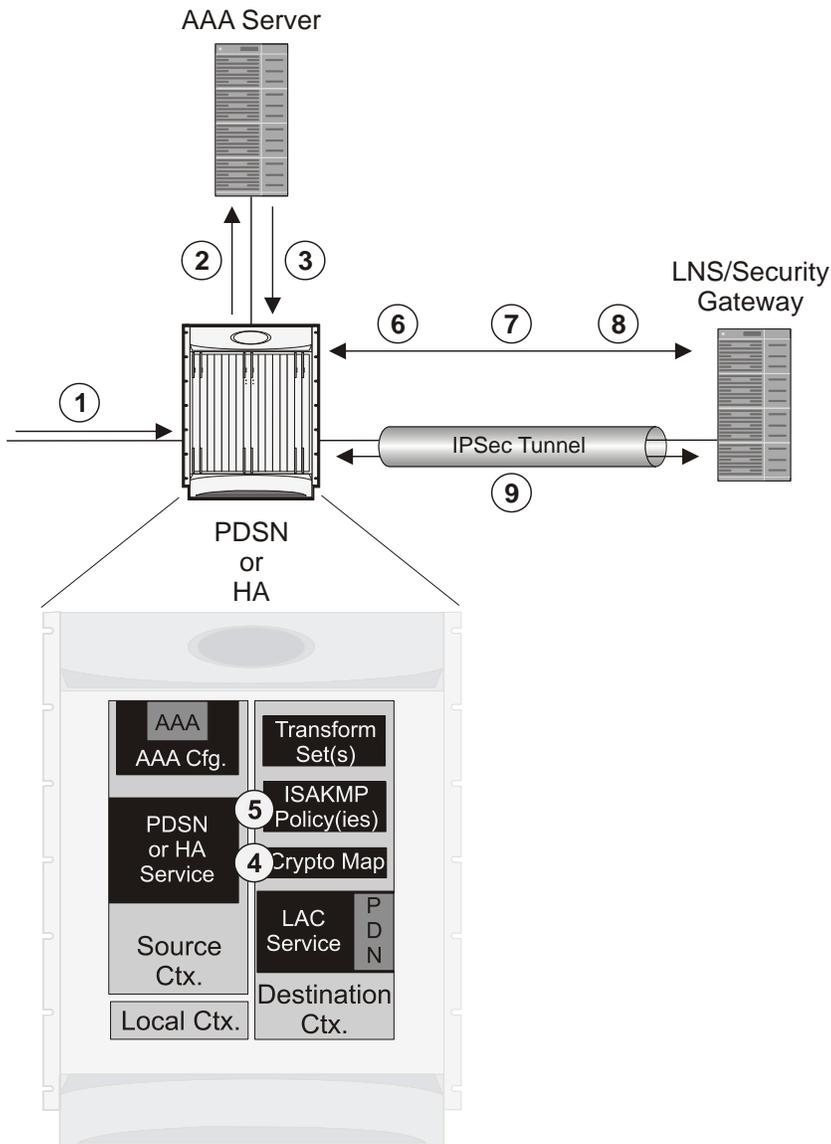


Table 25. Attribute-based L2TP, IPsec-Encrypted Session Processing

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 39. PDSN Compulsory L2TP, IPsec-Encrypted Session Processing

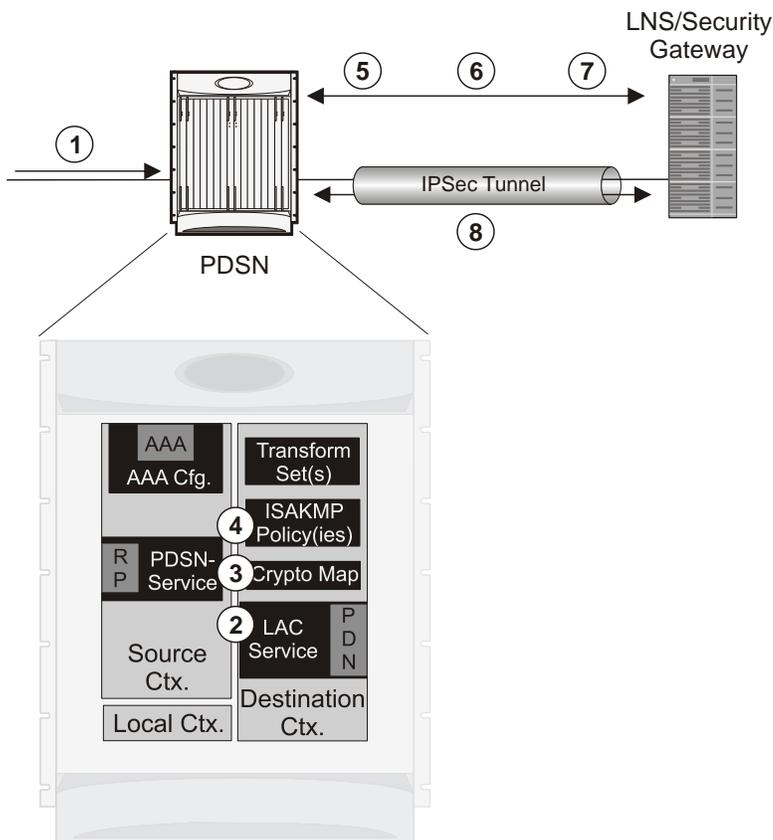


Table 26. PDSN Compulsory L2TP, IPsec-Encrypted Session Processing

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 40. GGSN PDP Context Processing with IPsec-Encrypted L2TP

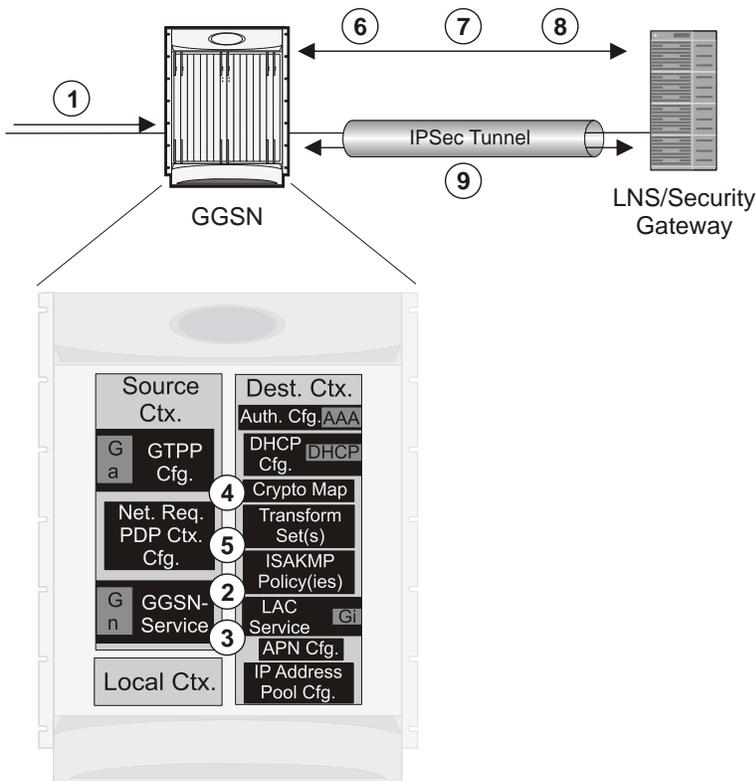


Table 27. GGSN PDP Context Processing with IPsec-Encrypted L2TP

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-abc | des-abc }
      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 <preshared_secret> ]

        isakmp default crypto-map <map_name> [ secret <preshared_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 <preshared_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 cryptop 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.
- *<lns\_address>* is IP address of the LNS 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 cryptot 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- ISAKMP- 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- ISAKMP- 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 41. X.509 Certificate-based Peer Authentication

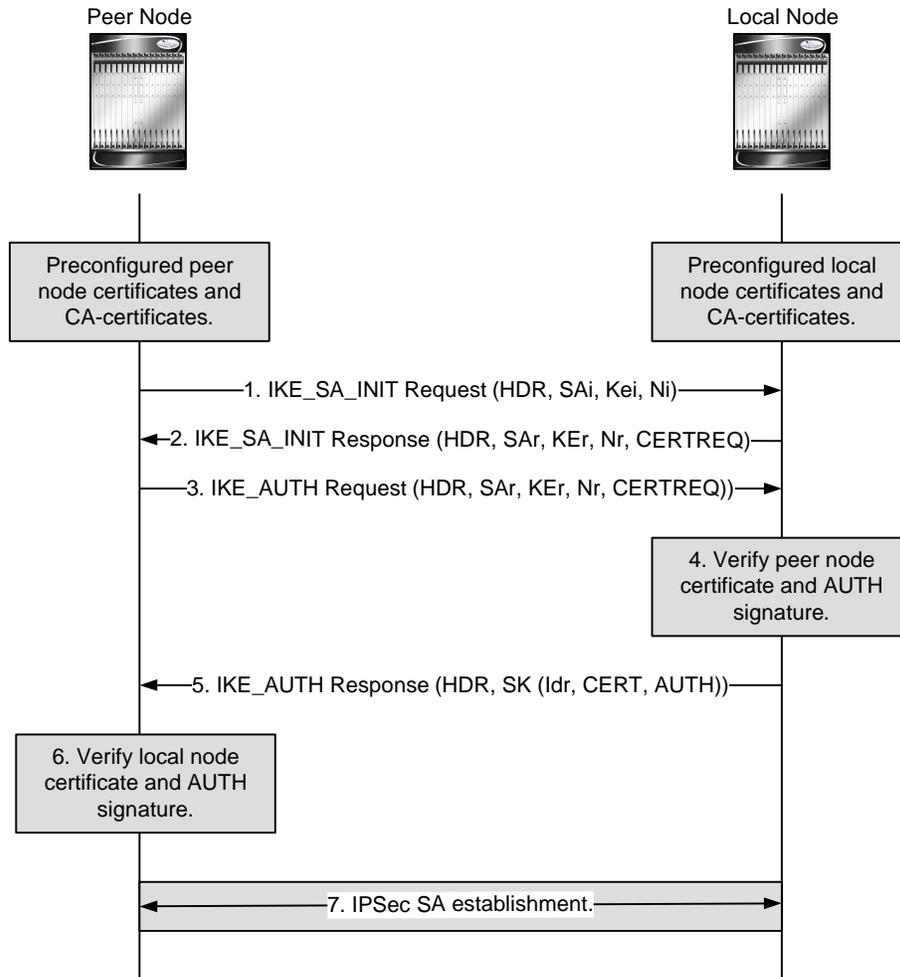


Table 30. X.509 Certificate-based Peer Authentication

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 42. E-UTRAN/EPC Logical Network Interfaces Supporting IPSec Tunnels

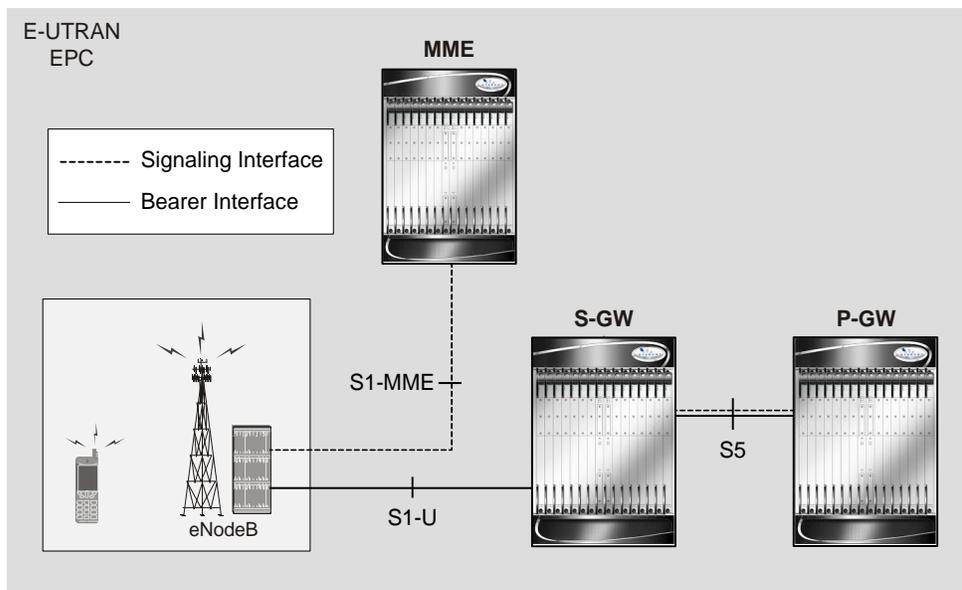


Table 31. E-UTRAN/EPC Logical Network Interfaces Supporting IPSec Tunnels

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 G

## 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>

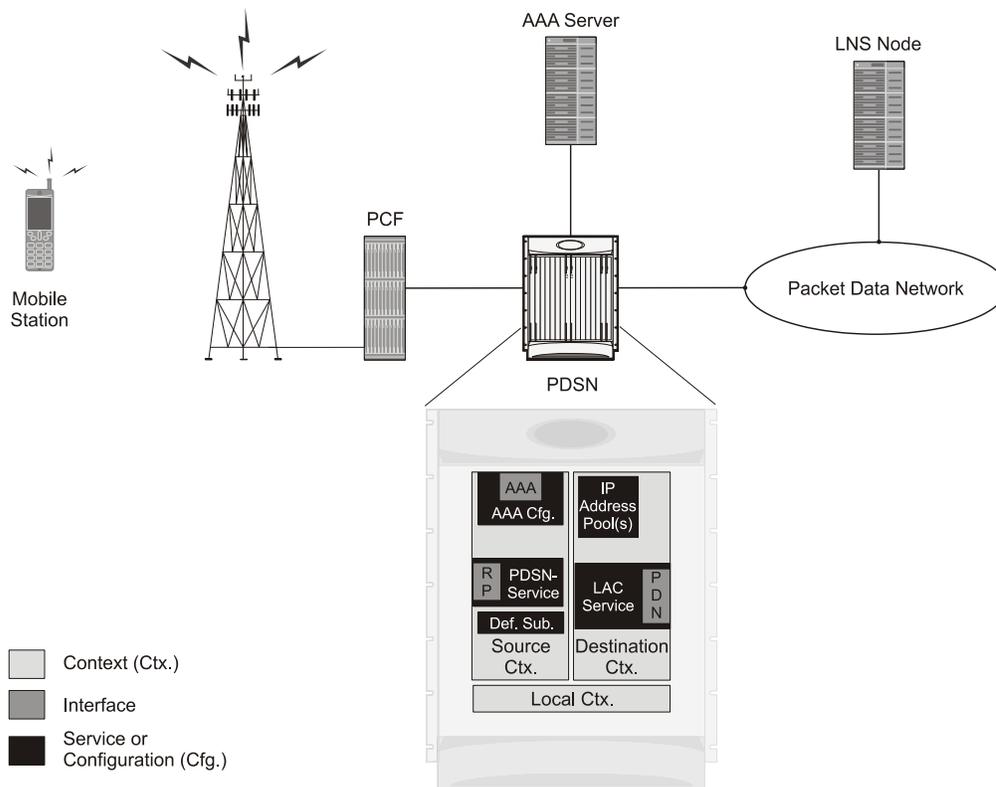
## Supported LAC Service Configurations for PDSN Simple IP

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 43. LAC Service Configuration for SIP



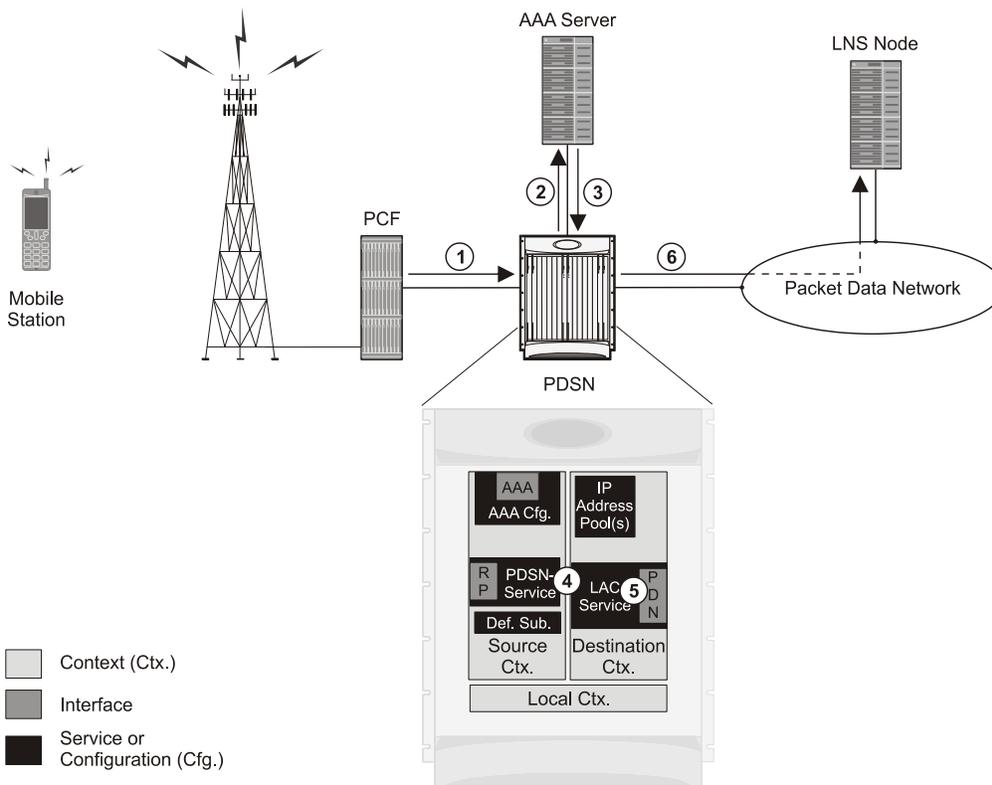
## Attribute-based Tunneling

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 44. 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

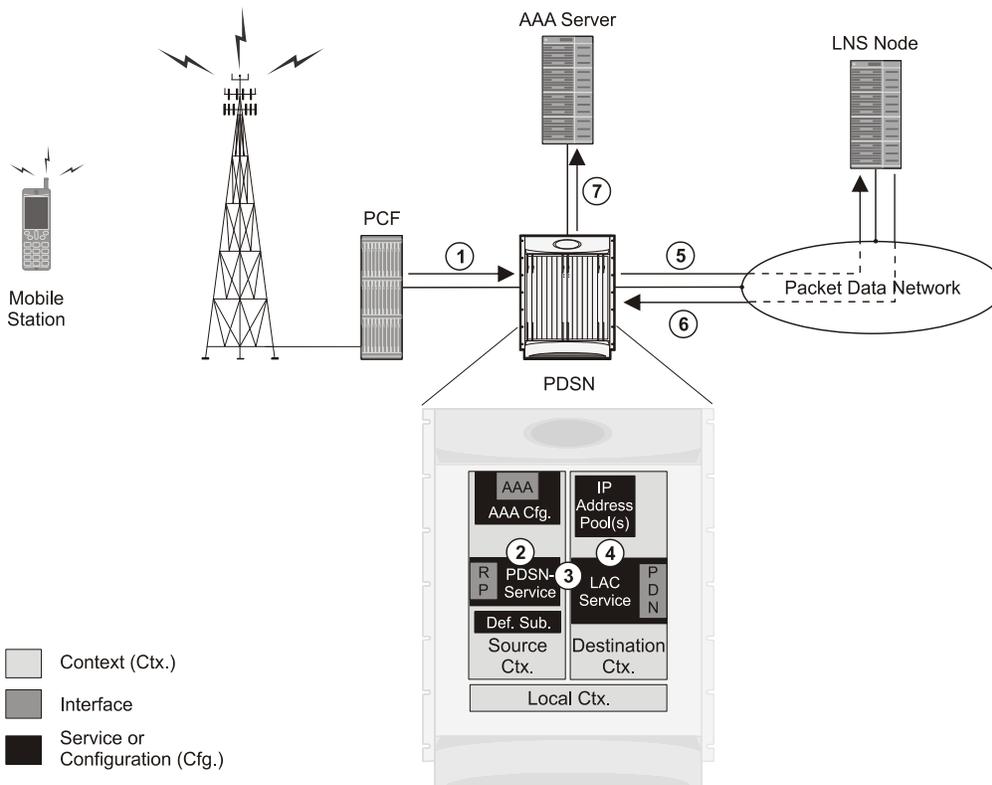
PDSN Service-based compulsory tunneling enables wireless operators to send all PPP traffic to remote LNS peers over an L2TP tunnel for authentication. This means that no PPP authentication is performed by the system.

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 45. 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.

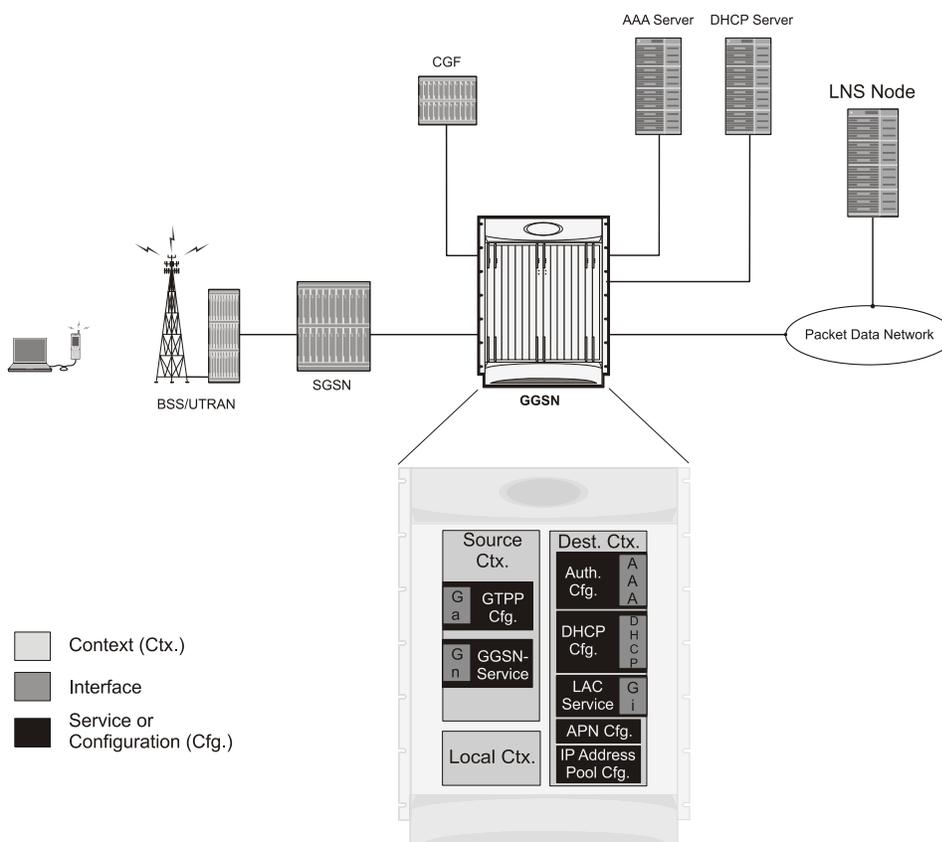
**Important:** These instructions assume that the system was previously configured to support subscriber data sessions as a PDSN.

- 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 46. 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:

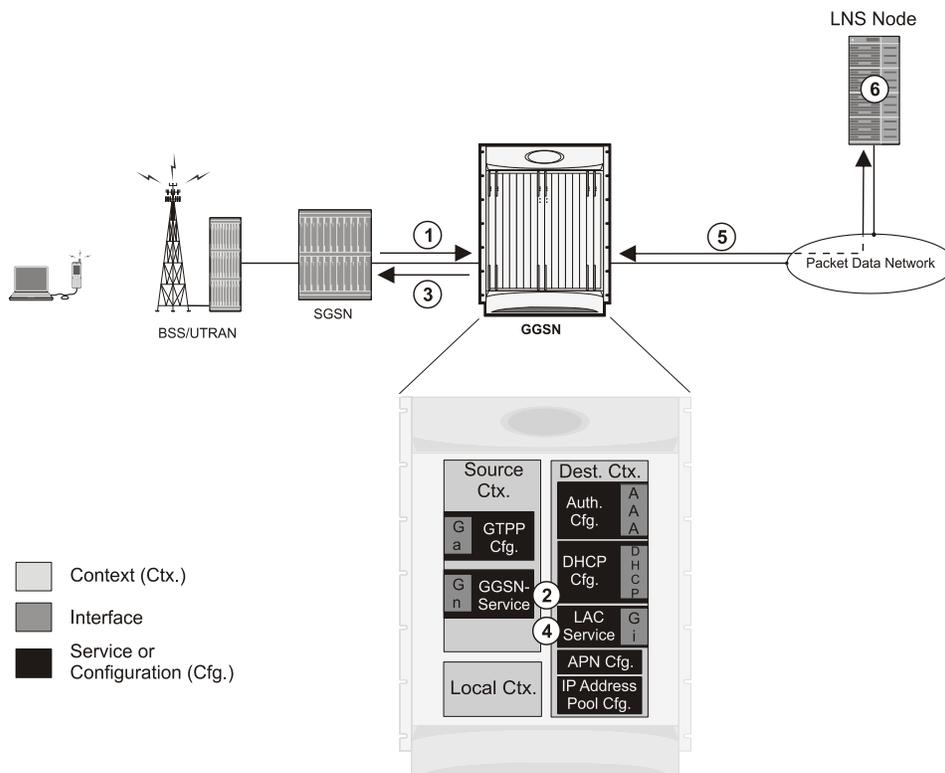
- **Transparent IP:** The APN template's L2TP parameter settings will be applied to the session.
- **Non-transparent IP:** Since authentication is required, L2TP parameter attributes in the subscriber profile (if configured) will take precedence over the settings in the APN template.
- **PPP:** The APN 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 47. 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

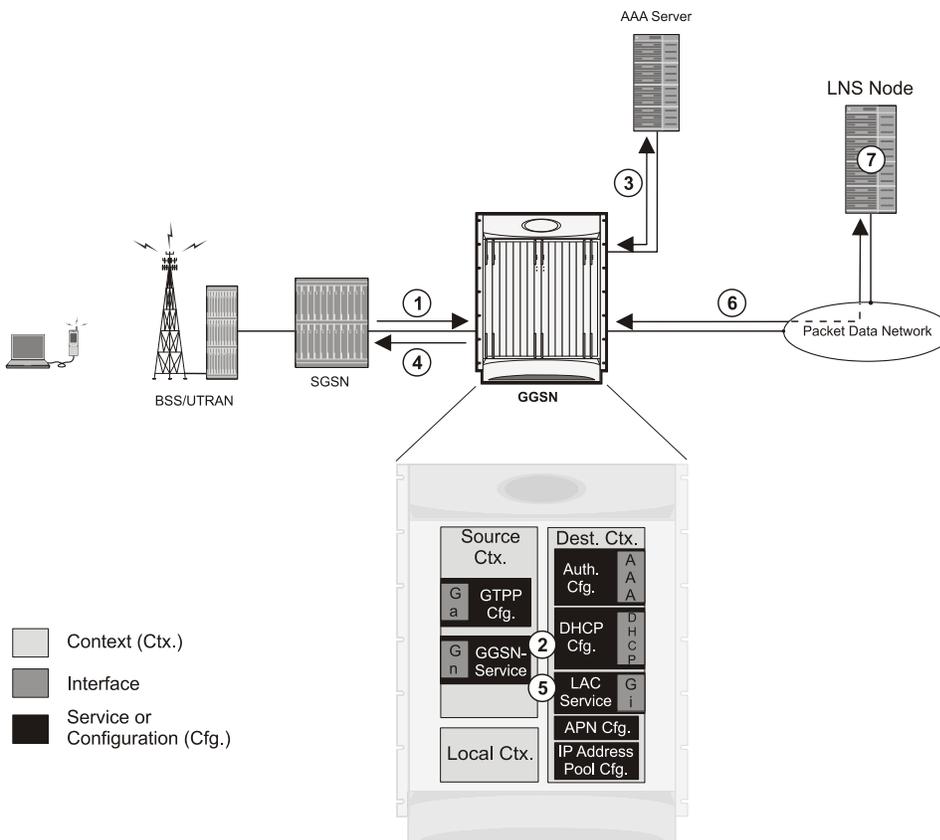
sessions. If no outbound information is configured, the subscriber's International Mobile Subscriber Identity (IMSI) is used as the username at the peer LNS.

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 48. 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.

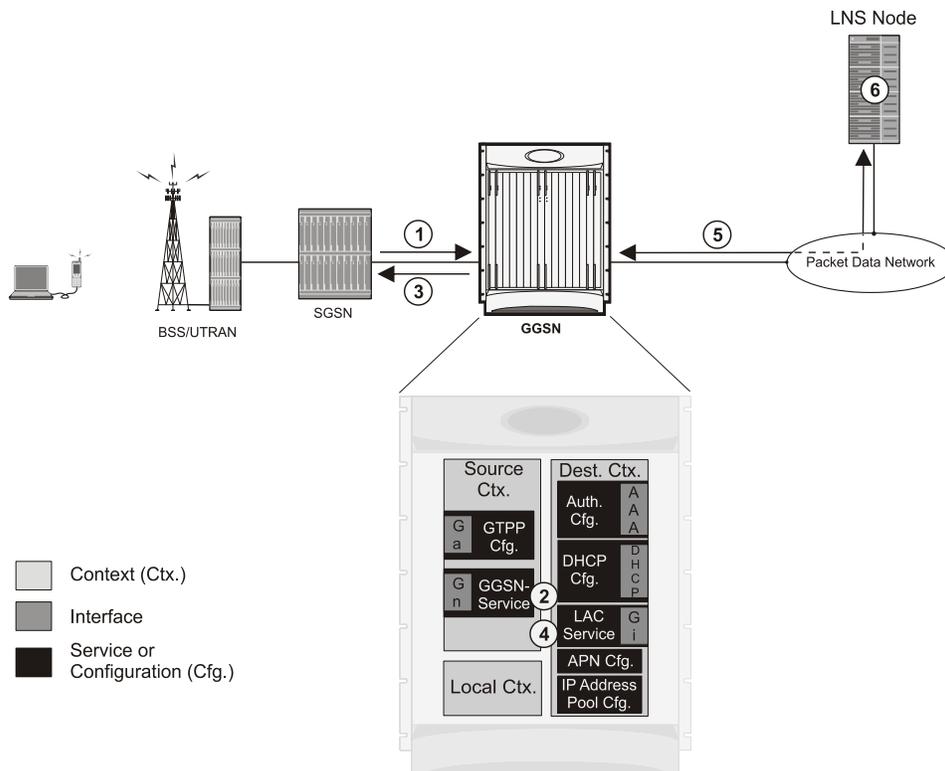
If these attributes are supplied, they take precedence over those specified in the APN template.

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 49. 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.

---

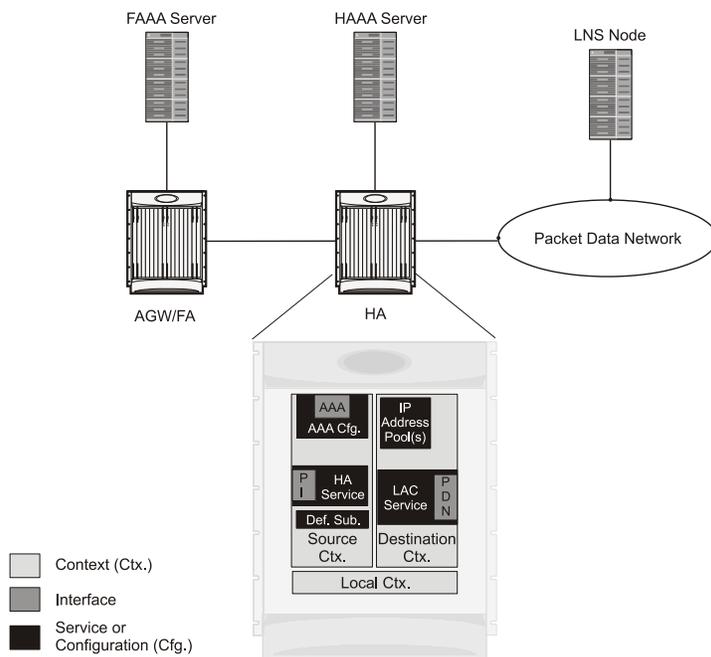
2. Configure one or more LAC services according to the information and instructions located in the *Configuring LAC Services* section of this chapter.
3. Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command `save configuration`. For 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.

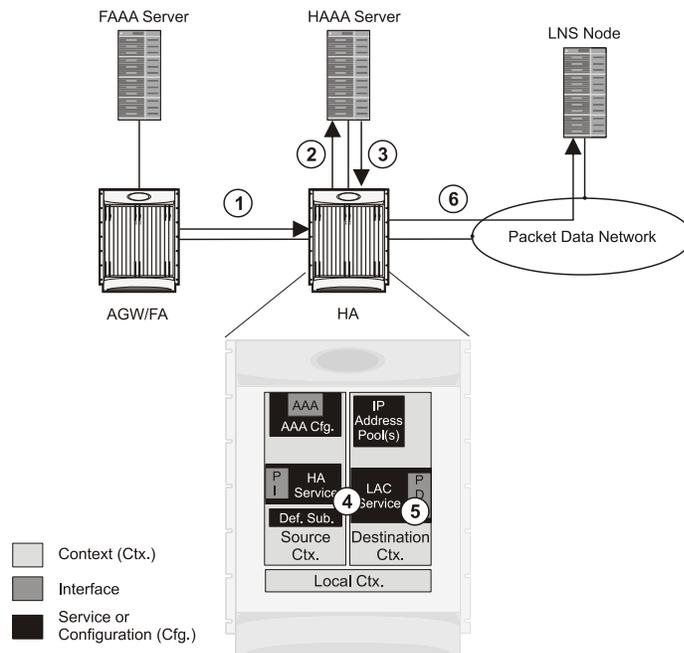
Figure 50. LAC Service Configuration for MIP



## 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 51. 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 unencapsulated.

## 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.   <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.
- <lms\_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 H

## 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 I

## 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 33. 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 52. AAA/PDSN Assigned IP Address Proxy Mobile IP Call Flow

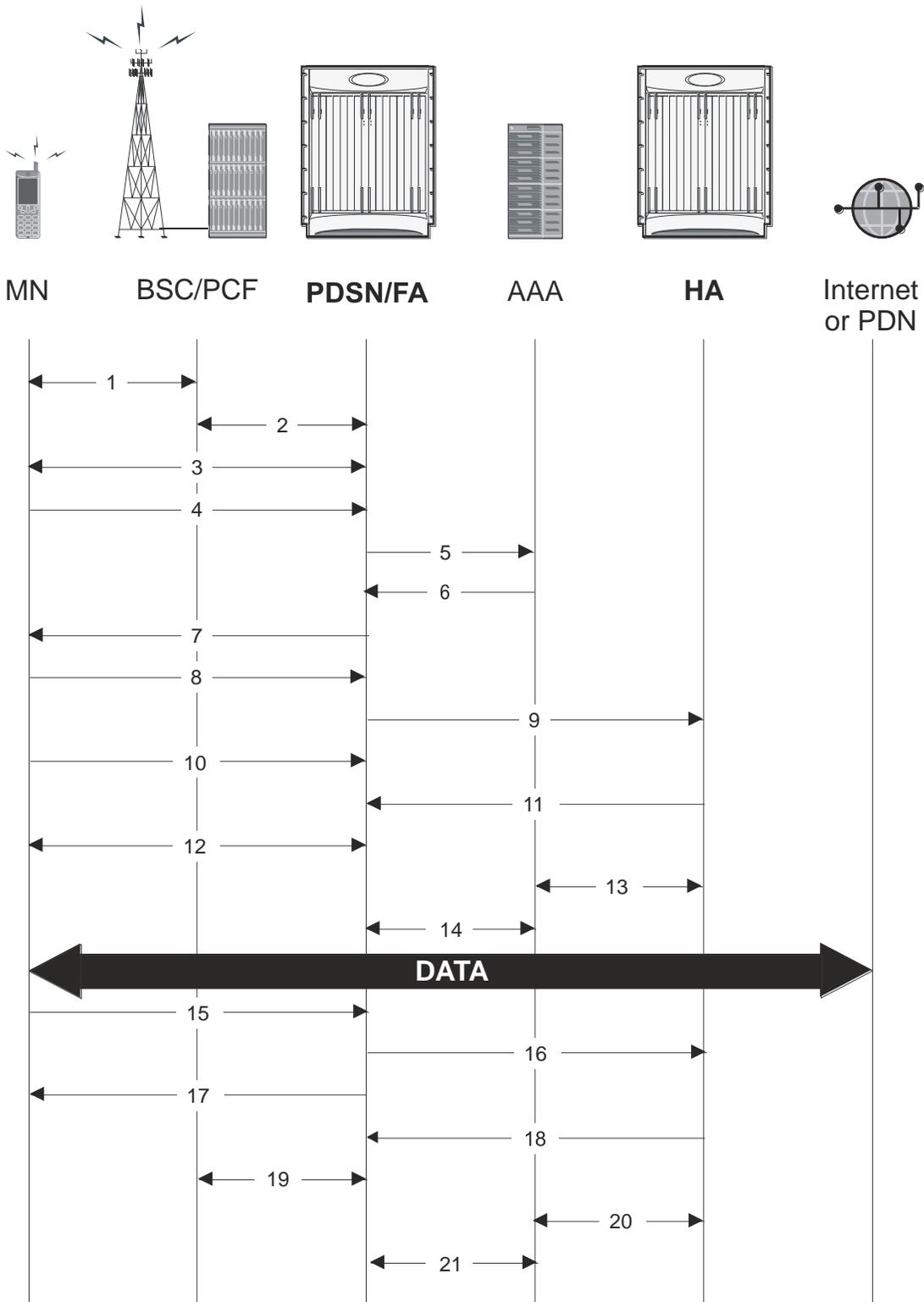


Table 34. AAA/PDSN Assigned IP Address Proxy Mobile IP Call Flow Description

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 53. HA Assigned IP Address Proxy Mobile IP Call Flow

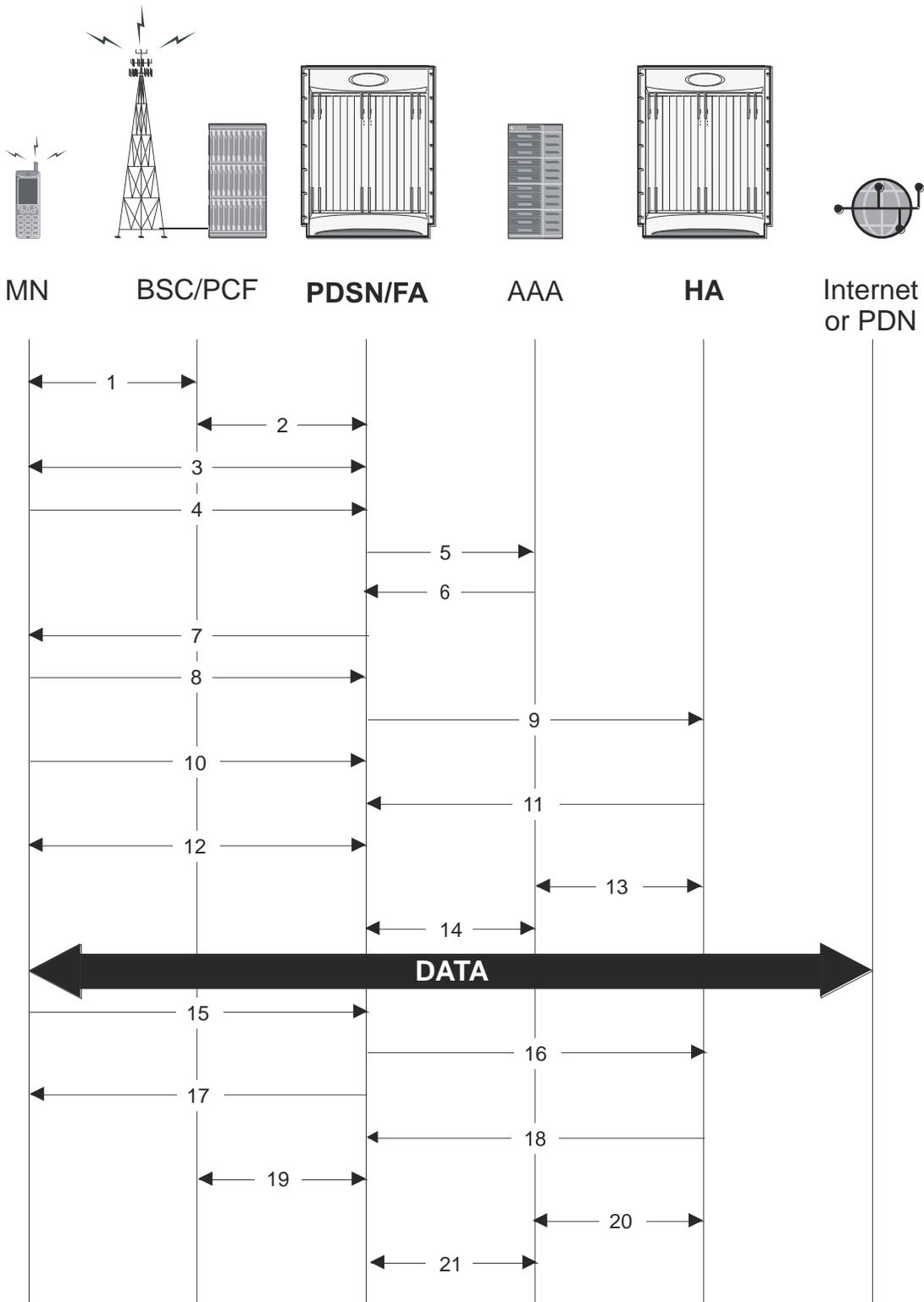


Table 35. HA Assigned IP Address Proxy Mobile IP Call Flow Description

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 54. Proxy Mobile IP Call Flow in 3GPP

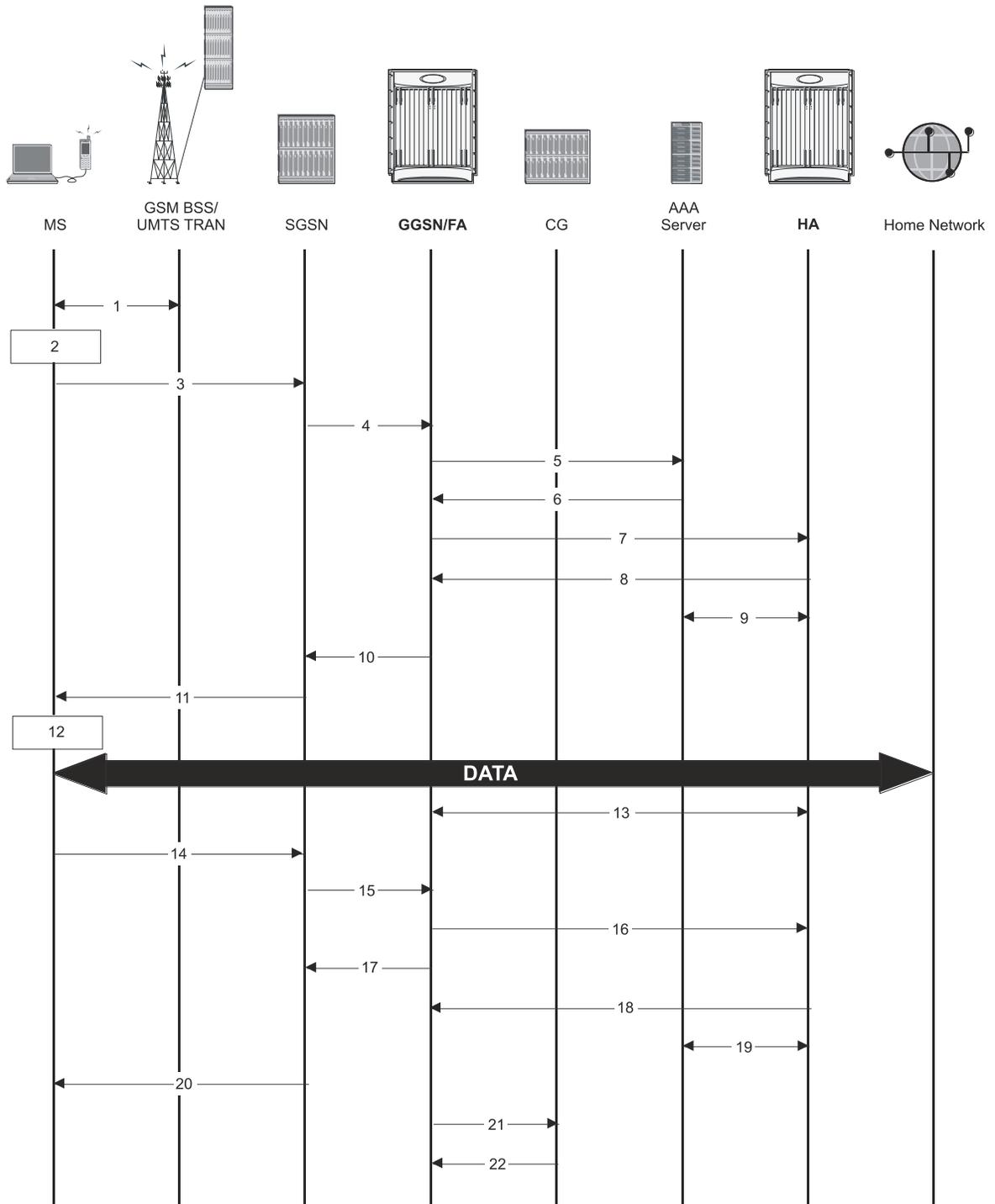


Table 36. Proxy Mobile IP Call Flow in 3GPP Description

Step	Description
------	-------------

Step	Description
1	The mobile station (MS) goes through the process of attaching itself to the GPRS/UMTS network.
2	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 signalling 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 a AAA server.
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	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.

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 55. AAA/ASN GW Assigned IP Address Proxy Mobile IP Call Flow

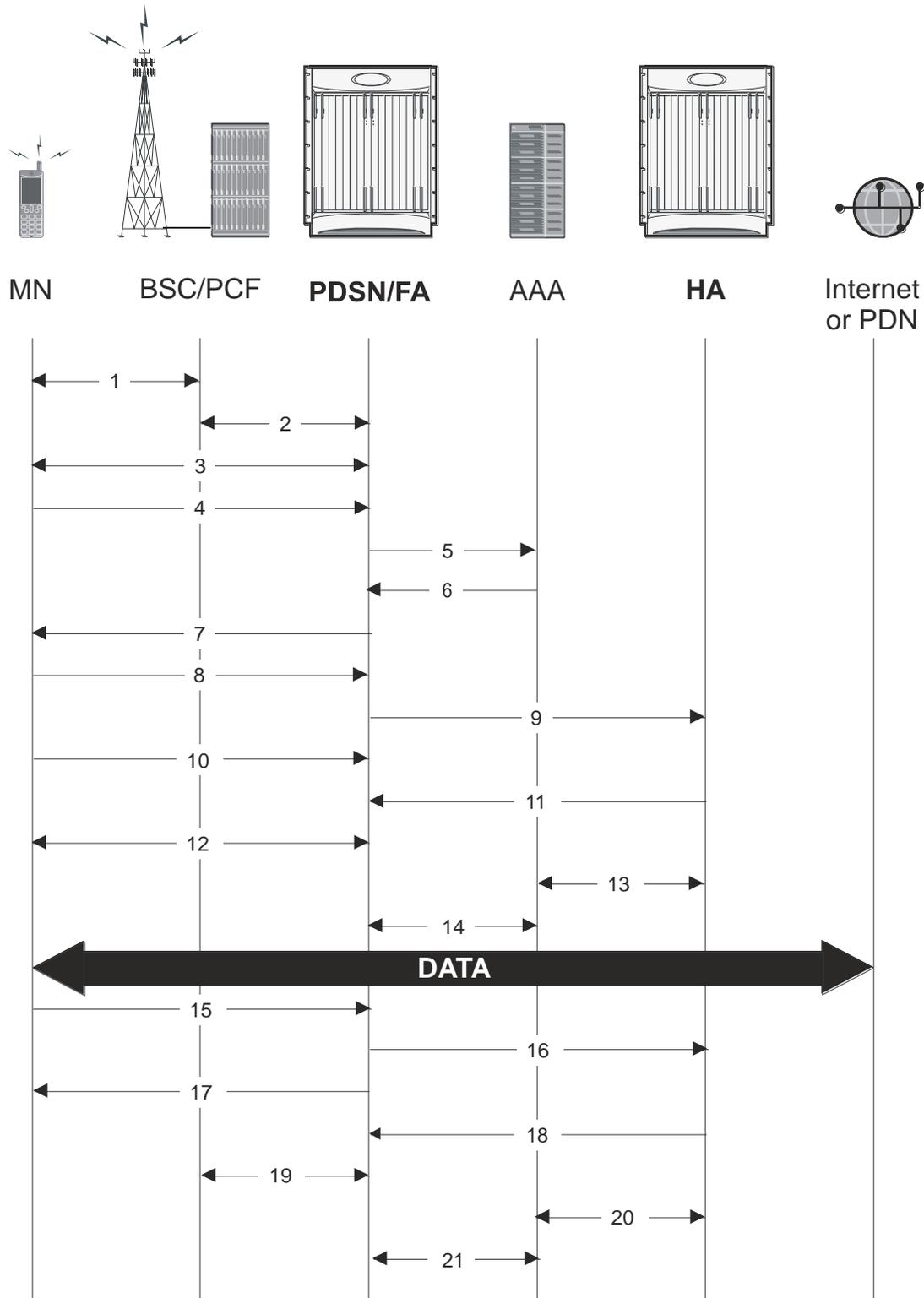


Table 37. AAA/ASN GW Assigned IP Address Proxy Mobile IP Call Flow Description

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 56. HA Assigned IP Address Proxy Mobile IP Call Flow

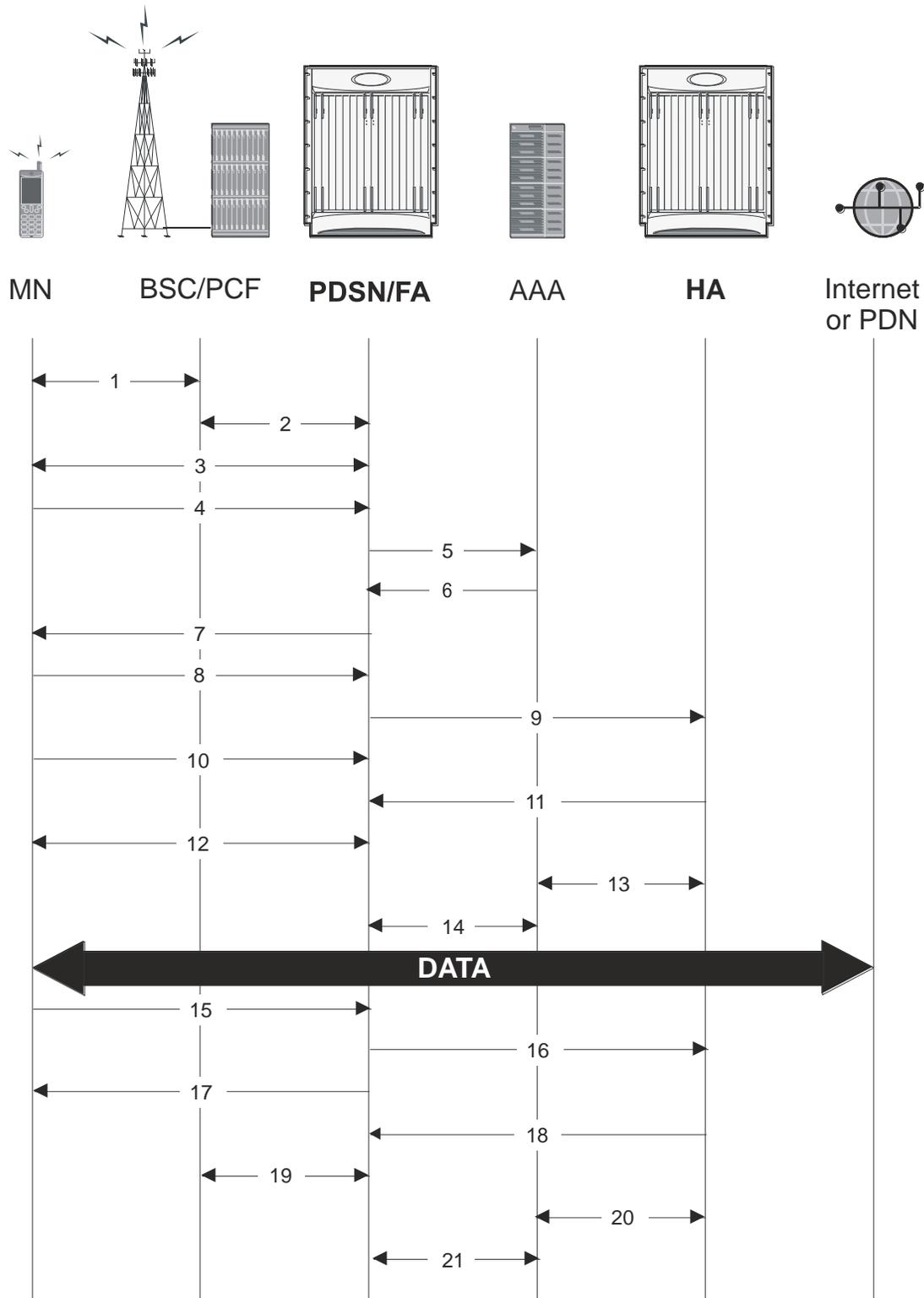


Table 38. HA Assigned IP Address Proxy Mobile IP Call Flow Description

Step	Description
1	Mobile Node (MN) secures a traffic channel over the airlink with the 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 57. Proxy-MIP Call Setup using CHAP Authentication

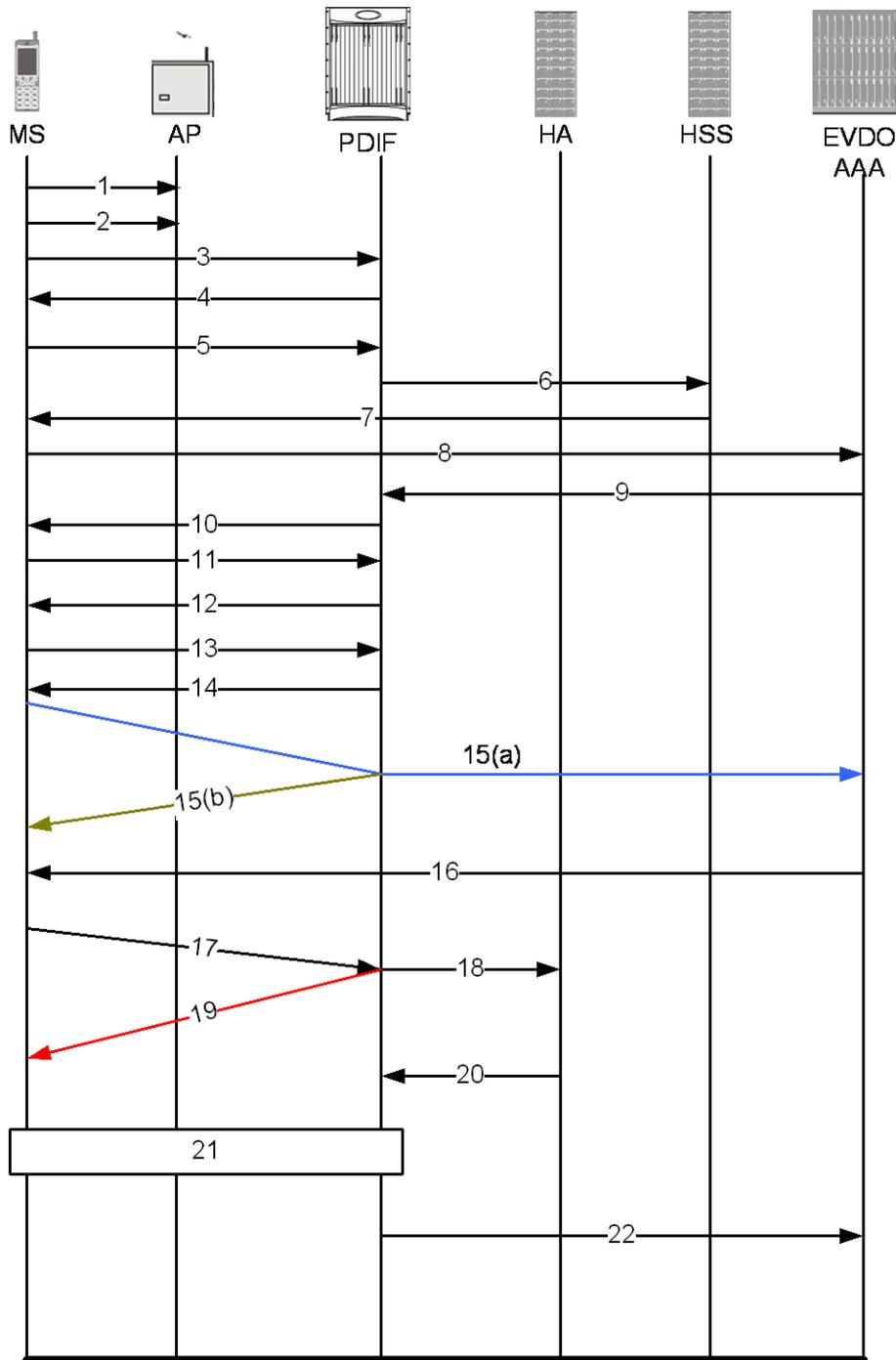


Table 39. Proxy-MIP Call Setup using CHAP Authentication

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, TSi, 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.  b. If the configured method is EAP-GTC, PDIF sends the IKE_AUTH Response with EAP-GTC.  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.  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	<p>PDIF receives Access Accept from RADIUS and sends IKE_AUTH Response with EAP success.</p>
17	<p>PDIF receives the final IKE_AUTH Request with AUTH payload.</p>
18	<p>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.</p>
19	<p>If <b>proxy-mip-required</b> is disabled, PDIF assigns the IP address from the local pool.</p>
20	<p>PDIF received proxy-MIP RRP and gets the IP address and DNS addresses.</p>
21	<p>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.</p>
22	<p>PDIF sends a RADIUS Accounting start message.</p>



**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 58. Proxy-MIP Call Setup using PAP Authentication

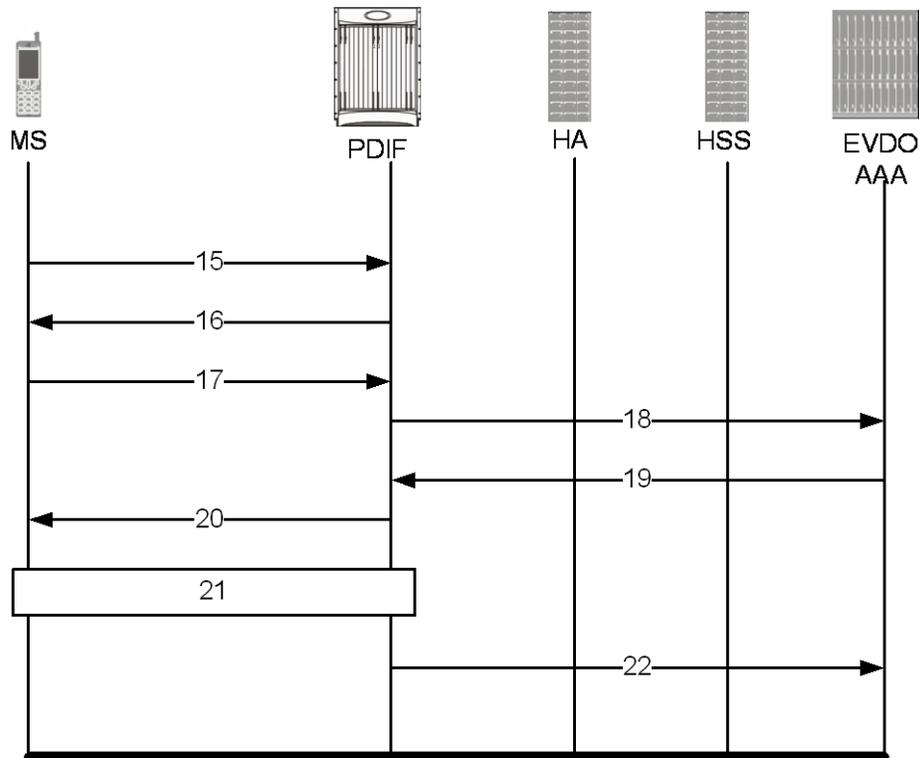


Table 40. Proxy-MIP Call Setup using PAP Authentication

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 41. 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 enables 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. <code>apn_name</code> 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 J

## 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 42. 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
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
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 43. 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 44. 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 45. 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)	<p>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.</p> <p>This attribute can be sent multiple times for different traffic classes. If Class is set to 0, it applies across all traffic classes.</p>

# Appendix K

## Sample Configuration Files

---

This appendix contains sample configuration files for the P-GW. The following configurations are supported:

- [Standalone eGTP PDN Gateway](#)
- [Standalone PMIPv6 PDN Gateway Supporting an eHRPD Network](#)

In each configuration example, commented lines are labeled with the number symbol (#) and variables are identified using italics within brackets (<*variable*>).

# Standalone eGTP PDN Gateway

## Configuration Sample

```
# Configuration file for an ASR 5000 in an eGTP P-GW role
#
# Send P-GW licenses
configure /flash/flashconfig/<pgw_license_name>.cfg
end
#
# Set system to not require confirmation when creating new contexts
and/or services. Config file must end with "no autoconfirm" to return the
CLI to its default setting.
#
configure
    autoconfirm
#
# Configure ASR 5000 cards
#
# Activate the PSCs
    card <slot_number>
        mode active psc
    exit
    card <slot_number>
        mode active psc
    exit
# Repeat for the number of PSCs in the system
end
```

```
#
# Modify the local context for local system management
config
  context local
    interface <name>
      ip address <address> <mask>
      exit
    server ftpd
      exit
    ssh key <key> length <bytes>
    server sshd
      subsystem sftp
      exit
    server telnetd
      exit
    subscriber default
      exit
    administrator <name> encrypted password <password> ftp
    aaa group default
      exit
    administrator <name> encrypted password <password> ftp
    ip route <ip_addr/ip_mask> <next_hop_addr> <lcl_cntxt_intrfc_name>
    exit
  port ethernet <slot#/port#>
    no shutdown
    bind interface <lcl_cntxt_intrfc_name> local
    exit
  ntp
    enable
```

```
server <ip_address>
exit

snmp engine-id local <id>

snmp notif-threshold <count> low <low_count> period <seconds>

snmp authentication-failure-trap

snmp heartbeat interval <minutes>

snmp community <string> read-write

snmp target <name> <ip_address>

system contact <string>

system location <string>

# P-GW context configuration

gtp single-source

context <pgw_context_name>

    interface <s5s8_interface_name>

        ip address <ipv4_address>

# note alternative IPv6 address:

    ipv6 address <address>

    exit

gtp group default

    gtp charging-agent address <gx_ipv4_address>

    gtp echo-interval <seconds>

    gtp attribute diagnostics

    gtp attribute local-record-sequence-number

    gtp attribute node-id-suffix <string>

    gtp dictionary <name>

    gtp trigger egcdr max-losdv

    gtp egcdr losdv-max-containers <number>

    gtp server <ipv4_address> priority <num>

    gtp server <ipv4_address> priority <num> node-alive enable
```

```
exit

policy accounting <rf_policy_name> -noconfirm

    accounting-level {level_type}

    accounting-event-trigger interim-timeout action stop-start

    operator-string <string>

    cc profile <index>

exit

subscriber default

    exit

apn <rf_acct_apn_name>

    accounting-mode radius-diameter

    associate accounting-policy <rf_policy_name>

    ims-auth-service <gx_ims_service_name>

    aaa group <rf-radius_group_name>

    dns primary <ipv4_address>

    dns secondary <ipv4_address>

    ip access-group <name> in

    ip access-group <name> out

    mediation-device context-name <pgw_context_name>

    ip context-name <pdn_context_name>

    ipv6 access-group <name> in

    ipv6 access-group <name> out

    active-charging rulebase <name>

exit

aaa group <gz_acct_apn_name>

    bearer-control-mode mixed

    selection-mode sent-by-ms

    accounting-mode gtp

    gtp group default accounting-context <aaa_context_name>
```

```
ims-auth-service <gx_ims_service_name>
ip access-group <name> in
ip access-group <name> out
ip context-name <pdn_context_name>
active-charging rulebase <gz_rulebase_name>
exit

aaa group default
radius attribute nas-ip-address address <ipv4_address>
radius accounting interim interval <seconds>
diameter authentication dictionary <name>
diameter accounting dictionary <name>
diameter authentication endpoint <s6b_cfg_name>
diameter accounting endpoint <rf_cfg_name>
diameter authentication server <s6b_cfg_name> priority <num>
diameter accounting server <rf_cfg_name> priority <num>
exit

egtp-service <egtp_service_name> -noconfirm
interface-type interface-pgw-ingress
validation-mode default
associate gtpu-service <gtpu_service_name>
gtpc bind address <s5s8_interface_ip_address>
exit

gtpu-service <gtpu_service_name>
bind ipv4-address <s5s8_interface_ip_address>
# note alternative IPv6 address:
bind ipv6-address <s5s8_interface_ip_address>
exit

pgw-servers <pgw_service_name> -noconfirm
associate egtp-service <egtp_service_name>
```

```
    associate qci-qos-mapping <name>

    fqdn host <domain_name> realm <realm_name>

    plmn id mcc <id> mnc <id>

    exit

    ipv6 route <ipv6_addr/prefix> next-hop <sgw_addr> interface <pgw_sgw_intrfc_name>

    exit

port ethernet <slot_number/port_number>

    no shutdown

    bind interface <s5s8_interface_name> <pgw_context_name>

    exit

# PDN context configuration

context <pdn_context_name> -noconfirm

    interface <pdn_sgi_ipv4_interface_name>

        ip address <ipv4_address>

        exit

    interface <pdn_sgi_ipv6_interface_name>

        ipv6 address <address>

        exit

    ip pool <name> range <start_address end_address> public <priority>

    ipv6 pool <name> range <start_address end_address> public <priority>

    subscriber default

    ip access-list <name>

        redirect css service <name> any

        permit any

        exit

    ipv6 access-list <name>

        redirect css service <name> any

        permit any

        exit
```

```
aaa group default
    exit
exit
port ethernet <slot_number/port_number>
    no shutdown
    bind interface <pdn_ipv4_interface_name> <pdn_context_name>
    exit
port ethernet <slot_number/port_number>
    no shutdown
    bind interface <pdn_ipv6_interface_name> <pdn_context_name>
    exit
# Enabling active charging
require active-charging optimized-mode
active-charging service <name>
    ruledef <name>
        <rule_definition>
        .
        .
        <rule_definition>
    exit
    ruledef default
        ip any-match = TRUE
    exit
    ruledef icmp-pkts
        icmp any-match = TRUE
    exit
    ruledef qci3
        icmp any-match = TRUE
    exit
```

```
ruledef static
    icmp any-match = TRUE
    exit
charging-action <name>
    <action>
    .
    .
    <action>
    exit
charging-action icmp
    billing-action egcdr
    exit
charging-action qci3
    content-id <id>
    billing-action egcdr
    qos-class-identifier <id>
    allocation-retention-priority <priority>
    tft-packet-filter qci3
    exit
charging-action static
    service-identifier <id>
    billing-action egcdr
    qos-class-identifier <id>
    allocation-retention-priority <priority>
    tft-packet-filter qci3
    exit
rulebase default
    exit
rulebase <name>
```

```

    <rule_base>
        .
        .
    <rule_base>
    exit

rulebase <gx_rulebase_name>

    dynamic-rule order first-if-tied

    egcdr tariff minute <minute> hour <hour>(optional)

    billing-records egcdr

    action priority 5 dynamic-only ruledef qci3 charging-action qci3
    action priority 100 ruledef static charging-action static
    action priority 500 ruledef default charging-action icmp
    action priority 570 ruledef icmp-pkts charging-action icmp

    egcdr threshold interval <interval>

    egcdr threshold volume total <bytes>

    exit

exit

# AAA and policy

    context <aaa_context_name> -noconfirm

        interface <gx_interface_name>

            ipv6 address <address>

# note alternative IPv4 address:

            ip address <ipv4_address>

            exit

        interface <gy_interface_name>

            ipv6 address <address>

# note alternative IPv4 address:

            ip address <ipv4_address>

            exit

```

```

interface <gz_interface_name>
    ip address <ipv4_address>
    exit

interface <rf_interface_name>
    ip address <ipv4_address>

# note alternative IPv6 address:
    ipv6 address <address>
    exit

subscriber default
    exit

ims-auth-service <gx_ims_service_name>
    p-cscf discovery table <#> algorithm round-robin
    p-cscf table <#> row-precedence <#> ipv6-address <pcrf_ipv6_adr>

# note alternative IPv4 address:
    p-cscf table <#> row-precedence <#> ip-address <pcrf_ipv4_adr>

policy-control
    diameter origin endpoint <gx_cfg_name>
    diameter dictionary <name>
    diameter host-select table <#> algorithm round-robin
    diameter host-select row-precedence <#> table <#> host <gx_cfg_name>
    exit

exit

diameter endpoint <gx_cfg_name>
    origin realm <realm_name>
    origin host <name> address <aaa_context_ip_address>
    peer <gx_cfg_name> realm <name> address <pcrf_ip_addr>
    route-entry peer <gx_cfg_name>
    exit

diameter endpoint <gy_cfg_name>

```

```
    origin realm <realm_name>

    origin host <name> address <aaa_context_ip_address>

    peer <gy_cfg_name> realm <name> address <ocs_ip_addr>

    route-entry peer <gy_cfg_name>

    exit

diameter endpoint <rf_cfg_name>

    origin realm <realm_name>

    origin host <name> address <aaa_context_ip_address>

    peer <rf_cfg_name> realm <name> address <ofcs_ip_addr>

    route-entry peer <rf_cfg_name>

    exit

exit

port ethernet <slot_number/port_number>

    no shutdown

    bind interface <gx_interface_name> <aaa_context_name>

    exit

port ethernet <slot_number/port_number>

    no shutdown

    bind interface <gy_interface_name> <aaa_context_name>

    exit

port ethernet <slot_number/port_number>

    no shutdown

    bind interface <gz_interface_name> <aaa_context_name>

    exit

port ethernet <slot_number/port_number>

    no shutdown

    bind interface <rf_interface_name> <aaa_context_name>

    exit

# QCI-QoS mapping
```

```
qci-qos-mapping <name>
  qci 1 user-datagram dscp-marking <hex>
  qci 3 user-datagram dscp-marking <hex>
  qci 9 user-datagram dscp-marking <hex>
end
```

# Standalone PMIPv6 PDN Gateway Supporting an eHRPD Network

## Configuration Sample

```
# Configuration file for an ASR 5000 in a PMIPv6 P-GW role supporting an eHRPD network
#
# Send P-GW licenses
configure /flash/flashconfig/<pgw_license_name>.cfg
end
#
# Set system to not require confirmation when creating new contexts
and/or services. Config file must end with "no autoconfirm" to return the
CLI to its default setting.
#
configure
    autoconfirm
#
# Configure ASR 5000 cards
#
# Activate the PSCs
    card <slot_number>
        mode active psc
    exit
    card <slot_number>
        mode active psc
    exit
# Repeat for the number of PSCs in the system
end
```

```
#
# Modify the local context for local system management
config
  context local
    interface <name>
      ip address <address> <mask>
      exit
    server ftpd
      exit
    ssh key <key> length <bytes>
    server sshd
      subsystem sftp
      exit
    server telnetd
      exit
    subscriber default
      exit
    administrator <name> encrypted password <password> ftp
    aaa group default
      exit
    administrator <name> encrypted password <password> ftp
    ip route <ip_addr/ip_mask> <next_hop_addr> <lcl_cntxt_intrfc_name>
    exit
  port ethernet <slot#/port#>
    no shutdown
    bind interface <lcl_cntxt_intrfc_name> local
    exit
  ntp
    enable
```

```
server <ip_address>
exit

snmp engine-id local <id>

snmp notif-threshold <count> low <low_count> period <seconds>

snmp authentication-failure-trap

snmp heartbeat interval <minutes>

snmp community <string> read-write

snmp target <name> <ip_address>

system contact <string>

system location <string>

# P-GW context configuration

context <pgw_context_name>

interface <s2a_interface_name>

    ipv6 address <ipv6_address>

        tunnel-mode ipv6ip

            source interface <name>

            destination address <ipv4_or_ipv6_address>

        exit

    exit

exit

policy accounting <rf_policy_name> -noconfirm

    accounting-level {level_type}

    accounting-event-trigger interim-timeout action stop-start

    operator-string <string>

    exit

subscriber default

    exit

apn <name>

    accounting-mode radius-diameter
```

```
associate accounting-policy <rf_policy_name>

ims-auth-service <gx_ims_service_name>

aaa group <rf-radius_group_name>

dns primary <ipv4_address>

dns secondary <ipv4_address>

ip access-group <name> in

ip access-group <name> out

mediation-device context-name <pgw_context_name>

ip context-name <pdn_context_name>

ipv6 access-group <name> in

ipv6 access-group <name> out

active-charging rulebase <name>

exit

aaa group <rf-radius_group_name>

radius attribute nas-identifier <id>

radius accounting interim interval <seconds>

radius dictionary <name>

radius mediation-device accounting server <address> key <key>

diameter authentication dictionary <name>

diameter accounting dictionary <name>

diameter authentication endpoint <s6b_cfg_name>

diameter accounting endpoint <rf_cfg_name>

diameter authentication server <s6b_cfg_name> priority <num>

diameter accounting server <rf_cfg_name> priority <num>

exit

aaa group default

radius attribute nas-ip-address address <ipv4_address>

radius accounting interim interval <seconds>

diameter authentication dictionary <name>
```

```

diameter accounting dictionary <name>

diameter authentication endpoint <s6b_cfg_name>

diameter accounting endpoint <rf_cfg_name>

diameter authentication server <s6b_cfg_name> priority <num>

diameter accounting server <rf_cfg_name> priority <num>

exit

lma-service <lma_service_name> -noconfirm

no aaa accounting

revocation enable

bind address <s2a_interface_ipv6_address>

exit

pgw-service <pgw_service_name>

associate lma-service <lma_service_name>

associate qci-qos-mapping <name>

authorize external

plmn id mcc <id> mnc <id>

exit

ipv6 route <ipv6_addr/prefix> next-hop <sgw_addr> interface <pgw_sgw_intrfc_name>

exit

port ethernet <slot_number/port_number>

no shutdown

bind interface <s2a8_interface_name> <pgw_context_name>

exit

# PDN context configuration

context <pdn_context_name> -noconfirm

interface <pdn_sgi_ipv4_interface_name>

ip address <ipv4_address>

exit

interface <pdn_sgi_ipv6_interface_name>

```

```
    ipv6 address <address>
  exit

ip pool <name> range <start_address end_address> public <priority>
ipv6 pool <name> range <start_address end_address> public <priority>
subscriber default
  exit

ip access-list <name>
  redirect css service <name> any
  permit any
  exit

ipv6 access-list <name>
  redirect css service <name> any
  permit any
  exit

aaa group default
  exit

exit

port ethernet <slot_number/port_number>
  no shutdown
  bind interface <pdn_ipv4_interface_name> <pdn_context_name>
  exit

port ethernet <slot_number/port_number>
  no shutdown
  bind interface <pdn_ipv6_interface_name> <pdn_context_name>
  exit

# Enabling active charging
require active-charging optimized-mode
active-charging service <name>
  ruledef <name>
```

```
<rule_definition>
.
.
<rule_definition>
exit
ruledef <name>
<rule_definition>
.
.
<rule_definition>
exit
charging-action <name>
<action>
.
.
<action>
exit
charging-action <name>
<action>
.
.
<action>
exit
rulebase default
exit
rulebase <name>
<rule_base>
.
.
```

```
        <rule_base>
    exit

    exit

# AAA and policy

    context <aaa_context_name> -noconfirm

        interface <gx_interface_name>

            ipv6 address <address>

# note alternative IPv4 address:

            ip address <ipv4_address>

            exit

        interface <gy_interface_name>

            ipv6 address <address>

# note alternative IPv4 address:

            ip address <ipv4_address>

            exit

        interface <s6b_interface_name>

            ip address <ipv4_address>

# note alternative IPv6 address:

            ipv6 address <address>

            exit

        interface <rf_interface_name>

            ip address <ipv4_address>

# note alternative IPv6 address:

            ipv6 address <address>

            exit

    subscriber default

        exit

    ims-auth-service <gx_ims_service_name>

        p-cscf discovery table <#> algorithm round-robin
```

```

    p-cscf table <#> row-precedence <#> ipv6-address <pcrf_ipv6_adr>
# note alternative IPv4 address:
    p-cscf table <#> row-precedence <#> ip-address <pcrf_ipv4_adr>
policy-control
    diameter origin endpoint <gx_cfg_name>
    diameter dictionary <name>
    diameter host-select table <#> algorithm round-robin
    diameter host-select row-precedence <#> table <#> host <gx_cfg_name>
    exit
exit
diameter endpoint <gx_cfg_name>
    origin realm <realm_name>
    origin host <name> address <aaa_context_ip_address>
    peer <gx_cfg_name> realm <name> address <pcrf_ip_addr>
    route-entry peer <gx_cfg_name>
    exit
diameter endpoint <gy_cfg_name>
    origin realm <realm_name>
    origin host <name> address <aaa_context_ip_address>
    peer <gy_cfg_name> realm <name> address <ocs_ip_addr>
    route-entry peer <gy_cfg_name>
    exit
diameter endpoint <s6b_cfg_name>
    origin realm <realm_name>
    origin host <name> address <aaa_context_ip_address>
    peer <s6b_cfg_name> realm <name> address <3gpp_aaa_ip_addr>
    route-entry peer <s6b_cfg_name>
    exit
diameter endpoint <rf_cfg_name>

```

```
    origin realm <realm_name>

    origin host <name> address <aaa_context_ip_address>

    peer <rf_cfg_name> realm <name> address <ofcs_ip_addr>

    route-entry peer <rf_cfg_name>

    exit

exit

port ethernet <slot_number/port_number>

    no shutdown

    bind interface <gx_interface_name> <aaa_context_name>

    exit

port ethernet <slot_number/port_number>

    no shutdown

    bind interface <gy_interface_name> <aaa_context_name>

    exit

port ethernet <slot_number/port_number>

    no shutdown

    bind interface <s6b_interface_name> <aaa_context_name>

    exit

port ethernet <slot_number/port_number>

    no shutdown

    bind interface <rf_interface_name> <aaa_context_name>

    exit

# QCI-QoS mapping

qci-qos-mapping <name>

    qci 1 user-datagram dscp-marking <hex>

    qci 3 user-datagram dscp-marking <hex>

    qci 9 user-datagram dscp-marking <hex>

end
```



# Appendix L

## P-GW Engineering Rules

---

This appendix provides PDN Gateway-specific engineering rules or guidelines that must be considered prior to configuring the ASR 5x00 for your network deployment. General and network-specific rules are located in the appendix of the System Administration and Configuration Guide for the specific network type.

The following rules are covered in this appendix:

- [Interface and Port Rules](#)
- [P-GW Context and Service Rules](#)
- [P-GW Subscriber Rules](#)

# Interface and Port Rules

The rules discussed in this section pertain to the Ethernet 10/100 line card, the Ethernet 1000 line card and the four-port Quad Gig-E line card and the type of interfaces they facilitate, regardless of the application.

## S2a Interface Rules

This section describes the engineering rules for the S2a interface for communications between the Mobility Access Gateway (MAG) service residing on the HSGW and the Local Mobility Anchor (LMA) service residing on the P-GW.

### LMA to MAG

The following engineering rules apply to the S2a interface from the LMA service to the MAG service residing on the HSGW:

- An S2a interface is created once the IP address of a logical interface is bound to an LMA service.
- The logical interface(s) that will be used to facilitate the S2a interface(s) must be configured within an ingress context.
- LMA services must be configured within an ingress context.
- Depending on the services offered to the subscriber, the number of sessions facilitated by the S2a interface can be limited in order to allow higher bandwidth per subscriber.

## P-GW Context and Service 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.

---

- The system supports unlimited peer HSGWs or S-GWs addresses per P-GW.
  - The system maintains statistics for a maximum of 8192 peer HSGWs or S-GWs per P-GW service.
  - If more than 8192 HSGWs or S-GWs are attached, older statistics are identified and overwritten.
- The system maintains statistics for a maximum of 4096 peer P-GWs per HSGW or S-GW service.
- There are a maximum of 8 P-GW assignment tables per context and per chassis.
- The total number of entries per table and per chassis is limited to 256.

## P-GW Subscriber Rules

The following engineering rule applies to subscribers configured within the system:

- Default subscriber templates may be configured on a per P-GW service.